UNC UAI Universidad Nacional de Córdoba

UNIDAD DE AUDITORIA INTERNA FOLIO 1 U.N.C.

INFORME DE AUDITORÍA Nº 23/16

Proyecto:

SISTEMAS INFORMATICOS

Área Auditada:

SISTEMA ADMINISTRATIVO SIU-DIAGUITA

Al Señor Rector de la
Universidad Nacional de Córdoba
Dr. Hugo Oscar Juri
S / D

Diciembre/2016

UNC UAI Universidad Nacional de Córdoba

UNIDAD DE AUDITORIA INTERNA FOLIO 2 U.N.C.

TABLA DE CONTENIDOS

UNC UAI Universidad Nacional de Córdoba

UNIDAD DE AUDITORIA INTERNA FOLIO 3 U.N.C.

INFORME EJECUTIVO

Proyecto: **SISTEMAS INFORMATICOS**
Informe N° **23/2016**
Área Auditada: **Secretaría de Gestión Institucional (SGI)**

Informe Ejecutivo

El presente informe tiene por objeto sintetizar el resultado de las tareas llevadas a cabo a fin de realizar un relevamiento y análisis de los controles implementados por la Secretaria de Gestión Institucional sobre el Sistema Informático SIU-DIAGUITA – sistema de gestión de Compras, Contrataciones y Patrimonio -.

La labor de auditoría fue realizada de acuerdo con los Normas de Auditoría Interna Gubernamental, aplicándose los procedimientos allí enumerados.
En esta oportunidad se utilizó un cuestionario como guía de trabajo.

Las labores de campo se llevaron a cabo en la 1ª quincena de Diciembre en La Dirección General de Tecnología Informática, y en la Dirección de Equipamiento Redes y Seguridad Informática.

El período cubierto por el examen alcanzó las operaciones realizadas en el 2° semestre del año 2016. El universo de transacciones revisadas, fue de un semestre y comprendieron el 100% de las mismas en el periodo señalado.

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.

A continuación se detallan las principales observaciones detectadas a partir de la aplicación de la Ord. HCS N° 03/2008:

SISTEMA ADMINISTRATIVO SIU-DIAGUITA

Procesamiento / Operaciones
No se pudo verificar el cumplimiento de los siguientes aspectos:

1) No existe un procedimiento documentado y aprobado de generación de backups (copias de resguardo). - *Cap. 8.4.1 Resguardo de la Información*.

2) No se ha especificado el responsable por la generación de los backups. - *Cap. 8.4.1 Resguardo de la Información.*

3) No se prueban los procedimientos de backups y su recuperación en forma periódica, para garantizar que se cumplan con los requerimientos de los planes de continuidad de las actividades. - *Cap. 8.4.1 Resguardo de la Información.*

4) No se asigna a los backups un nivel de protección física y ambiental adecuado. - *Cap. 7.6. Ubicación y Protección de Activos físicos.*

El incumplimiento de lo establecido en la ordenanza citada, provoca un descuido en el control del resguardo del Sistema.

Monitoreo de Actividades

No se pudo verificar el cumplimiento de los siguientes aspectos:

5) No se ha de designado formalmente un responsable del monitoreo del registro de actividades o logs. con el fin de analizar periódicamente los logs, y documentar los resultados. - *Cap. 8.4.2. Registro de Actividades del Personal Operativo. Y Cap. 8.4.3. Registro de Fallas.*

6) No existe un procedimiento de registro y control de actividades de los usuarios respecto del uso del sistema. - *Cap. 9.2.5. Revisión de Derechos de Acceso de Usuarios.*

7) No se realizan análisis periódicos de los logs de actividades. - *Cap. 9.7. Monitoreo del Acceso y Uso de los Sistemas.*

Esta situación debilita la seguridad y responsabilidades en la administración de la seguridad del sistema.

Registro de Operaciones y Otros Controles

No se pudo verificar el cumplimiento de los siguientes aspectos:

8) No existe un procedimiento formal definido y documentado para la puesta en producción del sistema o de nuevas versiones, asignando formalmente las responsabilidades para tal fin, con la verificación de la correcta implementación de los cambios, y diseñando los mecanismos necesarios, para que los técnicos y los usuarios, tomen conocimiento de

los cambios que brinda el sistema ante la implementación de nuevas versiones. *Cap. - 8.2.Planificación y Aprobación de Sistemas.*

El incumplimiento de lo establecido en la ordenanza citada, provoca una omisión en las Políticas de seguridad aplicadas al Sistema.

De las Observaciones detalladas se desprenden las siguientes Recomendaciones:

- En cuanto a los Procesamiento / Operaciones, se deberá considerar cada una de las observaciones expuestas en los puntos 1 al 4, con el fin de lograr un mejor y más eficiente control en el resguardo del Sistema.
- Se deberá implementar los Monitoreos de Actividades mencionados en los puntos 5 al 7 de las observaciones, con el fin de mejorar la continua optimización de los controles y, fortalecer el aprovechamiento del sistema SIU-DIAGUITA.
- Se deberá implementar en los Registros de Operaciones y Otros Controles la observación mencionada en el puntos 8, con el fin de mejorar los controles en la implementación de nuevas versiones.

Las Observaciones planteadas fueron analizadas por los funcionarios responsables, comprometiéndose a la implementación de las soluciones pertinentes, presentando su opinión y plan de acción de las mismas

Conclusión

Como conclusión de la presente Auditoría se puede apreciar que, el Sistema SIU-DIAGUITA se encuentra instalado para todas las Dependencias de la Universidad, que cuentan con un eficiente funcionamiento tanto en el Módulo Compras y Contrataciones como así también en el Módulo Patrimonio.
A los fines de acrecentar las medidas de seguridad del Sistema de Administración SIU-DIAGUITA es necesario que se cumplan con las Recomendaciones consignadas precedentemente.

Córdoba, 29 de Diciembre de 2016

An.S. SERGIO R. DIAZ
Auditor - U.A.I.
Universidad Nacional de Córdoba

Cra. LILIANA P. BOSAZ
Auditora Interna Titular
Universidad Nacional de Córdoba

UNC UAI Universidad Nacional de Córdoba

UNIDAD DE AUDITORIA INTERNA FOLIO 7 U.N.C.

INFORME ANALÍTICO

Proyecto: **SISTEMAS INFORMATICOS**
Informe Nº 23/**2016**
Área Auditada: **Secretaría de Gestión Institucional (SGI)**

Informe Analítico

I- OBJETO

Realizar una auditoría de los controles implementados por la Secretaria de Gestión Institucional sobre el Sistema Informático SIU-DIAGUITA – sistema de gestión de Compras, Contrataciones y Patrimonio -.

II- ALCANCE

La tarea de auditoría se llevó a cabo en la Secretaría de Gestión Institucional, más concretamente en la Dirección General de Tecnología Informática, y en la Dirección de Equipamiento Redes y Seguridad Informática. Las labores de campo se llevaron a cabo en la 1ª quincena de Diciembre.

Fue realizada de acuerdo con los Normas de Auditoría Interna Gubernamental, aplicándose los procedimientos allí enumerados.
En esta oportunidad se utilizó un cuestionario como guía de trabajo.

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.

III- MARCO DE REFERENCIA

El presente Informe se presenta en el marco del Plan de Trabajo del año 2016, y del desarrollo de Auditorías sobre Sistema Administrativos, correspondiente al Proyecto Sistemas Informáticos. La Auditoría se realizó en la Secretaría de Gestión Institucional.

Marco Normativo

Para la realización de la Auditoría se aplicó la Res.Nº48/05 SGN "Normas de Control Interno para Tecnología de la Información" y la Ord. HCS Nº03/08- "Política de Seguridad de la Información".

IV- TAREAS REALIZADAS Y PROCEDIMIENTOS APLICADOS

Se realizaron en las oficinas de la Secretaria de Gestión Institucional, específicamente en la Dirección General de Tecnología Informática, entrevistando a los responsables técnicos de los Módulos Compras y Contrataciones y del Módulo Patrimonio, con el fin de cumplimentar el cuestionario "PROGRAMA DE TRABAJO BASE SOBRE LOS CONTROLES INFORMÁTICOS DEL SISTEMA SIU-DIAGUITA" abarcando los temas Control de Accesos, Implementación del Sistema y Cambios a Programas, Procesamiento/Operaciones, Monitoreo de Actividades, Registro de Operaciones y otros Controles.

En la Dirección de Equipamiento Redes y Seguridad Informática se realizaron entrevistas con el fin de verificar todo lo ateniente al resguardo del sistema y procedimientos de copias del mismo.

Se adjunta en el Anexo I, copia del cuestionario realizado en la Secretaría de Gestión Institucional.

V- OBSERVACIONES, OPINIÓN DEL AUDITADO Y RECOMENDACIONES

A continuación se detallan las principales observaciones detectadas a partir de la aplicación de la Ord. HCS N° 03/2008:

Procesamiento / Operaciones

No se pudo verificar el cumplimiento de los siguientes aspectos:

1) No existe un procedimiento documentado y aprobado de generación de backups (copias de resguardo). - *Cap. 8.4.1 Resguardo de la Información.*

2) No se ha especificado el responsable por la generación de los backups. - *Cap. 8.4.1 Resguardo de la Información.*

3) No se prueban los procedimientos de backups y su recuperación en forma periódica, para garantizar que se cumplan con los requerimientos

de los planes de continuidad de las actividades. - *Cap. 8.4.1 Resguardo de la Información.*

4) No se asigna a los backups un nivel de protección física y ambiental adecuado. - *Cap. 7.6. Ubicación y Protección de Activos físicos.*

El incumplimiento de lo establecido en la ordenanza citada, provoca un descuido en el control del resguardo del Sistema.

Monitoreo de Actividades

No se pudo verificar el cumplimiento de los siguientes aspectos:

5) No se ha de designado formalmente un responsable del monitoreo del registro de actividades o logs. con el fin de analizar periódicamente los logs, y documentar los resultados. - *Cap. 8.4.2. Registro de Actividades del Personal Operativo. Y Cap. 8.4.3. Registro de Fallas.*

6) No existe un procedimiento de registro y control de actividades de los usuarios respecto del uso del sistema. - *Cap. 9.2.5. Revisión de Derechos de Acceso de Usuarios.*

7) No se realizan análisis periódicos de los logs de actividades. - *Cap. 9.7. Monitoreo del Acceso y Uso de los Sistemas.*

Esta situación debilita la seguridad y responsabilidades en la administración de la seguridad del sistema.

Registro de Operaciones y Otros Controles

No se pudo verificar el cumplimiento de los siguientes aspectos:

8) No existe un procedimiento formal definido y documentado para la puesta en producción del sistema o de nuevas versiones, asignando formalmente las responsabilidades para tal fin, con la verificación de la correcta implementación de los cambios, y diseñando los mecanismos necesarios, para que los técnicos y los usuarios, tomen conocimiento de los cambios que brinda el sistema ante la implementación de nuevas versiones. *Cap. - 8.2.Planificación y Aprobación de Sistemas.*

El incumplimiento de lo establecido en la ordenanza citada, provoca una omisión en las Políticas de seguridad aplicadas al Sistema.

OPINION DEL AUDITADO

Las Observaciones planteadas fueron aceptadas por los funcionarios responsables comprometiéndose a la implementación de las soluciones según consta en el CUDAP:EXP-UNC:0063583/2016.

Se ajuntan fotocopias de la documentación citada en el Anexo I.

RECOMENDACIONES

De las Observaciones detalladas se desprenden las siguientes Recomendaciones:

- En cuanto a los Procesamiento / Operaciones, se deberá considerar cada una de las observaciones expuestas en los puntos 1 al 4, con el fin de lograr un mejor y más eficiente control en el resguardo del Sistema.
- Se deberá implementar los Monitoreos de Actividades mencionados en los puntos 5 al 7 de las observaciones, con el fin de mejorar la continua optimización de los controles y, fortalecer el aprovechamiento del sistema SIU-DIAGUITA.
- Se deberá implementar en los Registros de Operaciones y Otros Controles la observación mencionada en el puntos 8, con el fin de mejorar los controles en la implementación de nuevas versiones.

VI- CONCLUSIONES

Como conclusión de la presente Auditoría se puede apreciar que, el Sistema SIU-DIAGUITA se encuentra instalado para todas las Dependencias de la Universidad, que cuentan con un eficiente funcionamiento tanto en el Módulo Compras y Contrataciones como así también en el Módulo Patrimonio.
A los fines de acrecentar las medidas de seguridad del Sistema de Administración SIU-DIAGUITA es necesario que se cumplan con las Recomendaciones consignadas precedentemente.

Córdoba, 29 de Diciembre de 2016

An.S. SERGIO R. DIAZ
Auditor - U.A.I.
Universidad Nacional de Córdoba

Cra. LILIANA P. BOSAZ
Auditora Interna Titular
Universidad Nacional de Córdoba

UNIDAD DE AUDITORIA INTERNA UNC FOLIO 12

AUDITORIA DE SISTEMAS INFORMATICOS

ANEXO I

DECANO	DIRECTOR INFORMATICA	AUDITOR
		An.S. SERGIO R. DIAZ Auditor - U.A.I. Universidad Nacional de Córdoba

PROGRAMA DE TRABAJO BASE SOBRE LOS CONTROLES INFORMÁTICOS DEL SISTEMA SIU-DIAGUITA

Universidad Nacional: Córdoba

Fecha: 02/12/16

	ASPECTO A VERIFICAR	CUMPLE			RIESGO			COMENTARIOS Y REFERENCIA A PAPELES DE TRABAJO
		Si	No	Parc.	Alto	Medio	Bajo	
1. CONTROL DE ACCESOS								
1.1	¿Existe uno o más Responsables del Sistema?	Si						4 Responsables.
1.2	¿Se definió un procedimiento documentado y aprobado para realizar las Altas, Bajas y Modificaciones (ABM) a los permisos de acceso al SIU-Diaguita?	Si						Res. 159 - Por Nota Electrónica (NE)
1.3	Súper Usuario, Autorizado para administrar el sistema. ¿Cuántos súper usuarios existen y quien los designa?	Si						1 en Compras 2 en Patrimonio
1.4	Esquema de autorización - ¿Qué son los Niveles y como se designa?	Si						Existen Dos Perfiles. Compras y Patrimonio
1.5	¿Se utilizan identificadores de usuario únicos (es decir, que identifican unívocamente a cada usuarios)?	Si						Es por Nº de CUIL -
1.6	¿Se ha entregado a los usuarios, un detalle escrito de sus derechos de acceso?		NO					Pero se desprende de la NE. que detalle el Perfil solicitado.
1.7	Dentro del esquema de autorización. ¿Qué son los Esquemas y como se los designa o tratan?	Si						Son prefijados por SIU - no fué necesario su modificación.
1.8	¿Se cancelan inmediatamente los derechos de acceso de los usuarios: • que cambiaron sus tareas, • a quienes se les revocó su autorización, • que se desvincularon de la Universidad?	Si						Se realiza pedido por intermedio de Nota Electrónica.
1.9	¿Se realizan controles especiales sobre las modificaciones de permisos de usuario?		NO					Es responsabilidad de los responsables en Dependencias.
1.10	¿Se efectúan revisiones periódicas sobre las cuentas de usuarios con el objeto de:							

UNIDAD DE AUDITORIA INTERNA UNC FOLIO 13

	ASPECTO A VERIFICAR	CUMPLE			RIESGO			COMENTARIOS Y REFERENCIA A PAPELES DE TRABAJO
		Si	No	Parc.	Alto	Medio	Bajo	
	• Cancelar identificadores y cuentas de usuario redundantes; • Inhabilitar cuentas inactivas por más de sesenta (60) días; • Eliminar cuentas inactivas por más de ciento veinte (120) días?	Si						Se controla mediante la primera migración. Posterior a eso No -
1.11	¿Se definieron los perfiles de acceso de usuarios estándar agrupados por categorías?	Si						Existen Perfiles estándar
1.12	El alcance de los perfiles (es decir, los permisos a otorgar en cada caso) ¿se determina en base a criterios documentados?	Si						Mediante Notas Electrónicas
1.13	¿Existe un procedimiento formal para la asignación de contraseñas?	Si						Es de Autogestion mediante Open ID.
1.14	¿Se suspende o bloquea permanentemente al usuario luego de tres (3) intentos de ingresar una contraseña incorrecta, siendo responsabilidad del usuario solicitar su rehabilitación al Responsable de Seguridad del Sistema?		NO					El sistema control de ingresos Open ID es el encargado de la Seguridad.
1.15	¿Se solicita a los usuarios el cambio periódico de la contraseña?	Si						Mediante Open ID.
1.16	¿Se toman los recaudos necesarios a fin de garantizar que los usuarios cambien -en su primer ingreso al sistema- las contraseñas iniciales que les son asignadas?		NO					No es nesario en Diaguita, lo administra Open ID
1.17	¿Existen procedimientos para la activación y desactivación del derecho de acceso al sistema?	Si						Mediante NE el usuario Pasa a estar Inactivo -
1.18	¿Se restringe el acceso directo a los datos por fuera del Sistema Diaguita?	Si						Esta protegido -
1.19	¿Se restringe a los usuarios la posibilidad de iniciar sesiones duplicadas?	Si						Con sesión controlado por tiempo de inactividad.
2. IMPLEMENTACIÓN DEL SISTEMA Y CAMBIOS A PROGRAMAS								
2.1	¿Existen procedimientos definidos para la puesta en producción de actualizaciones o nuevas versiones?	Si						No existe un procedimiento Autorizado -
2.2	¿Se registran las necesidades o requerimientos de modificaciones sobre el sistema?	Si						Se reciben Ticket en la comunidad SIU (GDE)
2.3	¿Existen pedidos de modificaciones pendientes?	Si						Son Mejoras -

UNIDAD DE AUDITORÍA INTERNA CNC FOLIO 14

	ASPECTO A VERIFICAR	CUMPLE			RIESGO			COMENTARIOS Y REFERENCIA A PAPELES DE TRABAJO
		Si	No	Parc.	Alto	Medio	Bajo	
2.4	¿Hay responsables técnicos del Sistema Informático, designados formalmente?		NO					No existe.
2.5	¿Existen mecanismos para que los técnicos y los usuarios, tomen conocimiento de los cambios que brinda el sistema ante la implementación de una nueva versión?	Si						Se comunican mediante mail.
2.6	Ante cada cambio de versión que lo requiera ¿se realiza una nueva capacitación y/o actualización?	Si						En algunos casos de Patrimonio se realizan reuniones.
2.7	¿Se verifica la correcta implementación de los cambios?	Si						
2.8	¿El usuario final forma parte del equipo que realiza los testeos luego de la implementación de cambios?	Si						
2.9	¿Se cuenta con un registro de control que contenga toda la información relevante de cada cambio o nueva versión implementada?	Si						En el control de Versionados figuran los cambios
2.10	¿Se realiza una revisión y monitoreo periódico del registro de cambios?	Si						
2.11	¿Se lleva a cabo una aprobación formal de los cambios o nuevas versiones que se implementan?	Si						Se reciben los distintos mail de los usuarios de control.
	3. PROCESAMIENTO / OPERACIONES							
3.1	El Sistema Diaguita ¿es el único utilizado para la registración de compras de bienes y servicios, y el control patrimonial de los bienes inventariables?	Si						
3.2	¿Está actualizada la implementación del SIU-Diaguita considerando la última versión disponible de acuerdo a lo informado por el SIU?	Si						V. 2.3.3
1 (3.3)	¿Se definió y documentó un procedimiento de generación de backups sobre la información del Sistema Diaguita?			Si				Existe una tabla de registro de conf's resguardo. En proceso de generación requerimiento de Backups.
3.4	¿El procedimiento contempla una periodicidad razonable para la generación de back ups?	Si						Cada hora
2 (3.5)	¿Está especificado el responsable por la generación de los							

UNIDAD DE AUDITORIA INTERNA UNC FOLIO 15

		ASPECTO A VERIFICAR	CUMPLE			RIESGO			COMENTARIOS Y REFERENCIA A PAPELES DE TRABAJO
			Si	No	Parc.	Alto	Medio	Bajo	
		backups?		NO					Res. SPGI 159/12 / 137/12
3	3.6	¿Se prueban los procedimientos de back up y su recuperación en forma periódica, para garantizar que cumplan con los requerimientos de los planes de continuidad de las actividades?		NO					
	3.7	¿Los medios de almacenamiento utilizados para los back ups son adecuadamente rotulados de modo de permitir su correcta identificación y administración?	Si						
	3.8	¿Existe un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo?	Si						
4	3.9	¿Se asigna a los back ups un nivel de protección física y ambiental adecuado?			Si				La localización de los servidores no son los correcto -
	3.10	¿Se mantiene una copia de back up en sitio externo, alejado del sitio de procesamiento?	Si						
	3.11	¿Se mantienen back ups de los programas y la configuración del Software Diaguita?	Si						
		4. MONITOREO DE ACTIVIDADES							
	4.1	¿Se encuentra un esquema de control de la base actual en funcionamiento?		No					
6	4.2	¿Existen procedimientos de registro y control de actividades de los usuarios respecto del uso del sistema?		NO					
	4.3	¿Se han definido las tareas críticas a registrar del sistema?	Si						control de estado de bienes.
	4.4	¿Se registran fecha, hora, identificación de usuario y terminal desde donde se realizan actividades críticas?		NO					
5	4.5	¿Se ha designado formalmente un responsable del monitoreo del registro de actividades o logs?		NO					
7	4.6	¿Se realizan análisis periódicos de los logs de actividades?		NO					
	4.7	¿Se documentan los resultados de los análisis periódicos de logs?		NO					

UNC UNIDAD DE AUDITORIA INTERNA FOLIO 16

	ASPECTO A VERIFICAR	CUMPLE			RIESGO			COMENTARIOS Y REFERENCIA A PAPELES DE TRABAJO
		Si	No	Parc.	Alto	Medio	Bajo	
5. SEPARACIÓN DE FUNCIONES, REGISTRO DE OPERACIONES Y OTROS CONTROLES								
5.1	¿Se registran las autorizaciones de cambios en las tablas/maestros del sistema?		NO					
5.2	En caso que las modificaciones de datos sobre las tablas/maestros sean descentralizadas ¿se realizan suficientes controles sobre los datos cargados por las unidades de gestión?		NO					Es Centralizado
5.3	La carga de datos sobre el sistema ¿se encuentra actualizada al día? ¿Funcionan on line?	Si						
5.4	¿Los accesos al Módulo "Migración", se encuentran otorgados únicamente al Administrador del Sistema?		NO					Movimientos Inciso 4, 2 etc Pasan a Pilagá - (ARAI)
5.5	Los usuarios ¿reciben cursos de capacitación y/o actualización para el uso del sistema? (es decir, aquellos usuarios que NO son referentes técnicos ni funcionales, a quienes el SIU brinda capacitaciones)	Si						Cursos de Patrimonio -
5.6	Los usuarios ¿disponen de acceso a los manuales del sistema?	Si						Mediante Actualización de Manuales por mail.
6. UNIVERSIDADES CON ESTRUCTURA DESCENTRALIZADA								
Los siguientes puntos son aplicables solo cuando el sistema SIU-DIAGUITA se utilice de forma descentralizada - Centralizado.								
6.1	Para la descentralización, ¿se siguió un procedimiento escrito que determine los roles a cumplir y la distribución de responsabilidades?							
6.2	En caso que se hubiera iniciado un proceso de descentralización: ¿Se documentó el Plan de Trabajo-Plan de Implementación? ¿Está aprobado?							
6.3	¿Se mantiene un registro de comunicación con las áreas descentralizadas? ¿Intervienen autoridades de las Unidades Administrativas?							
7.GENERACIÓN DE INFORMACIÓN GERENCIAL PARA OTROS SISTEMAS								
7.1	¿Existen procedimientos documentados para la generación de							

UNIDAD DE AUDITORIA INTERNA FOLIO 14

	ASPECTO A VERIFICAR	CUMPLE			RIESGO			COMENTARIOS Y REFERENCIA A PAPELES DE TRABAJO
		Si	No	Parc.	Alto	Medio	Bajo	
	información para otros sistemas?		NO					No se realizan
7.2	¿Están aprobados?							
7.3	¿Existe un responsable para autorizar la generación de información?							
7.4	¿La última generación de información fue hace más de 6 meses?							
7.5	¿Existe control sobre los datos registrados?							
8. INFORMACIÓN GENERADA POR OTROS SISTEMAS								
8.1	¿Existe una integración con otros sistemas?		NO					
8.2	¿Existe un responsable del control de los datos capturados por el SIU-Diaguita?							
8.3	¿Existe un procedimiento para detectar y resolver eventuales inconsistencias en la migración de datos de un sistema a otro?							
8.5	¿Se documenta la aprobación de la información generada/capturada?							
9. OTROS CONTROLES DEFINIDOS POR LA UAI								
	Se solicita copia de un archivo Log para su análisis.		NO					

Ing. LUCAS MANJARRÉS
Director de Equipamiento, Redes y Seg. Inf.
D G T I
Secretaría de Gestión Institucional

ING. OLGA CISNEROS
DGTI

Ing. Sonia Gelatti
Jefe Dpto. Soporte Eco-Fin Area Central-DGTI
Secretaría de Gestión Institucional

UNIDAD DE AUDITORIA INTERNA UNC FOLIO 48

UNIDAD DE AUDITORIA INTERNA
FOLIO
19
U.N.C

CUDAP: EXP-UNC:0063583/2016

Organismo: UNC

Datos de registración
Fecha y hora: 16-Dic-2016 10:59:45
Área: 55@unc - UNIDAD DE AUDITORÍA INTERNA

Datos de procedencia
Procedencia:
Número original:

Causante: UNIDAD DE AUDITORIA INTERNA

Responsable local	**Desde**
55@unc - UNIDAD DE AUDITORÍA INTERNA	16-Dic-2016 10:59:45

Título: SECRETARIA DE GESTIÓN INSTITUCIONAL - AUDITORIA INFORMÁTICA - OPINIÓN DEL AUDITADO

Texto

.

Fecha de impresión: 16-Dic-2016 10:59:45

CUDAP: EXP-UNC:0063583/2016

Rdo: 30/12/17.

UNC UAI Universidad Nacional de Córdoba

UNIDAD DE AUDITORIA INTERNA FOLIO 20 U.N.C.

UNIDAD DE AUDITORIA INTERNA FOLIO U.N.C.

Nota UAI Nº 98 /2016

Córdoba, 13 de Diciembre de 2016.-

Sr. Secretario de
Gestión Institucional
Mgter. Marcelo Adrián Sánchez
S / D

Me dirijo a Ud., y por su intermedio ante quien corresponda, a fin de elevar para su conocimiento, los hallazgos detectados en la auditoría informática iniciada el 22/11/2016 en esa Dependencia.

Asimismo, solicitamos tenga a bien manifestar en forma escrita su opinión al respecto, debiendo constar información clara y precisa referida al tiempo que estima le demandará la correspondiente regularización de todas y cada una de las observaciones de referencia, completando a tal efecto, el formulario "OPINION DEL AUDITADO Y PLAN DE ACCION", debidamente firmado por las autoridades que se detallan al pie del mismo.

El mencionado documento, deberá ser remitido a esta Unidad de Auditoría Interna, dentro del plazo máximo de 5 (cinco) días hábiles a contar de la fecha de recepción de la presente (según Normas de Auditoría Interna Gubernamental), para la continuación de los trámites inherentes ante la Superioridad Universitaria y la Sindicatura General de la Nación.

Sin otro particular saludo a Ud. atte.

An.S. SERGIO R. DIAZ
Auditor - U.A.I.
Universidad Nacional de Córdoba

UNC UAI Universidad Nacional de Córdoba

HALLAZGOS AUDITORIA INFORMATICA

SECRETARIA DE GESTIÓN INSTITUCIONAL

SISTEMA ADMINISTRATIVO SIU-DIAGUITA

Con el Objeto de realizar una verificación del sistema de control implementado por la Secretaria de Gestión Institucional sobre el Sistema Informático SIU-DIAGUITA – sistema de gestión de Compras, Contrataciones y Patrimonio -; se aplicó la Res.Nº48/05 SGN "Normas de Control Interno para Tecnología de la Información" y la Ord. HCS Nº03/08-"Política de Seguridad de la Información".

A continuación se detallan las Observaciones detectadas a partir de la aplicación de la Ord. HCS Nº03/2008:

Procesamiento / Operaciones
No se pudo verificar el cumplimiento de los siguientes aspectos:

1) No existe un procedimiento documentado y aprobado de generación de backups (copias de resguardo). - *Cap. 8.4.1 Resguardo de la Información.*

2) No se ha especificado el responsable por la generación de los backups. - *Cap. 8.4.1 Resguardo de la Información.*

3) No se prueban los procedimientos de backups y su recuperación en forma periódica, para garantizar que se cumplan con los requerimientos de los planes de continuidad de las actividades. - *Cap. 8.4.1 Resguardo de la Información.*

4) No se asigna a los backups un nivel de protección física y ambiental adecuado. - *Cap. 7.6. Ubicación y Protección de Activos físicos.*

Monitoreo de Actividades
No se pudo verificar el cumplimiento de los siguientes aspectos:

5) No se ha de designado formalmente un responsable del monitoreo del registro de actividades o logs, con el fin de analizar periódicamente los logs,

y documentar los resultados. - *Cap. 8.4.2. Registro de Actividades del Personal Operativo. Y Cap. 8.4.3. Registro de Fallas.*

6) No existe un procedimiento de registro y control de actividades de los usuarios respecto del uso del sistema. - *Cap. 9.2.5. Revisión de Derechos de Acceso de Usuarios.*

7) No se realizan análisis periódicos de los logs de actividades. - *Cap. 9.7. Monitoreo del Acceso y Uso de los Sistemas.*

Registro de Operaciones y Otros Controles

No se pudo verificar el cumplimiento de los siguientes aspectos:

8) No existe un procedimiento formal definido y documentado para la puesta en producción del sistema o de nuevas versiones, asignando formalmente las responsabilidades para tal fin, con la verificación de la correcta implementación de los cambios, y diseñando los mecanismos necesarios, para que los técnicos y los usuarios, tomen conocimiento de los cambios que brinda el sistema ante la implementación de nuevas versiones. *Cap. - 8.2.Planificación y Aprobación de Sistemas.*

UNC U.A.I.	FECHA 13/12/16	DEPENDENCIA: SECRETARIA DE GESTION INSTITUCIONAL	PROYECTO DE AUDITORIA SISTEMAS INFORMÁTICOS SIU-DIAGUITA	OPINION DEL AUDITADO Y PLAN DE ACCION

HALLAZGOS		OPINION	PLAN DE ACCION		
Nº	DETALLE		FECHA INICIO	FECHA FINAL	DETALLE
1	1) No existe un procedimiento documentado y aprobado de generación de backups (copias de resguardo).				
2	2) No se ha especificado el responsable por la generación de los backups.				
3	3) No se prueban los procedimientos de backups y su recuperación en forma periódica, para garantizar que se cumplan con los requerimientos de los planes de continuidad de las actividades.				
4	4) No se asigna a los backups un nivel de protección física y ambiental adecuado.				
5	5) No se ha de designado formalmente un responsable del monitoreo del registro de actividades o logs. con el fin de analizar periódicamente los logs, y documentar los resultados.				
6	6) No existe un procedimiento de registro y control de actividades de los usuarios respecto del uso del sistema.				
7	7) No se realizan análisis periódicos de los logs de actividades.				

UNIDAD DE AUDITORIA INTERNA UNC FOLIO 23

UNIDAD DE AUDITORIA INTERNA UNC FOLIO 4

8	8) No existe un procedimiento formal definido y documentado para la puesta en producción del sistema o de nuevas versiones, asignando formalmente las responsabilidades para tal fin, con la verificación de la correcta implementación de los cambios, y diseñando los mecanismos necesarios, para que los técnicos y los usuarios, tomen conocimiento de los cambios que brinda el sistema ante la implementación de nuevas versiones.				
		FIRMA Y ACLARACION DEL RESPONSABLE DEL PLAN DE ACCION			FIRMA DEL DECANO, DIRECTOR O SECRETARIO

UNIDAD DE AUDITORIA INTERNA UNC FOLIO 24

UNIDAD DE AUDITORIA INTERNA UNC FOLIO 5

UNC U.A.I.	FECHA 13/12/16	DEPENDENCIA: SECRETARIA DE GESTION INSTITUCIONAL	PROYECTO DE AUDITORIA SISTEMAS INFORMÁTICOS SIU-DIAGUITA	**OPINION DEL AUDITADO Y PLAN DE ACCION**

HALLAZGOS		OPINION	PLAN DE ACCION		
Nº	DETALLE		FECHA INICIO	FECHA FINAL	DETALLE
1	1) No existe un procedimiento documentado y aprobado de generación de backups (copias de resguardo).	Se cuenta con un registro de backups documentado en el sistema Intranet SGI que especifica periodicidad, metodología y datos a resguardar.	marzo/17	Agosto/17	* Creación de un formulario para que el propietario de la información (referente administrativo) lo complete en conjunto con DGTI, el cual contendrá las especificaciones del resguardo a realizar. * Documentación y formalización del procedimiento de backups del sistema SIU Diaguita en base al proceso actual de resguardo
2	2) No se ha especificado el responsable por la generación de los backups.	Según la Resol SPGI 137/12 en título "DGTI", Dirección de Equipamientos,Redes y Seguridad en las Funciones del "Departamento Equipamientos" y "Comunicaciones y Seguridad Informática" (pag 62 y 63) especifica el responsable de la planificación y generación de los backups.			
3	3) No se prueban los procedimientos de backups y su recuperación en forma periódica, para garantizar que se cumplan con los requerimientos de los planes de continuidad de las actividades.		marzo/17	Agosto/17	* Realización de procedimiento para recuperación y testeo de backups por los propietarios de la información. * Aprobación y formalización del procedimiento recuperación y testeo de backups del Siu Diaguita.
4	4) No se asigna a los backups un nivel de protección física y ambiental adecuado.	Actualmente solo se cuenta con almacenamientos en discos duros en los cuales se respaldan los datos de todos los sistemas y se encuentran al 90% de su capacidad. No es recomendable esta situación. No contamos con un lugar externo para resguardo de los backups.	marzo/17	Agosto/17	A través del expediente 63936/2016 se informó sobre varios aspectos vinculados a la seguridad de la información, encontrándose pendiente la solución que se intenta consensuar con la Prosecretaría de Informática. Se adjunta copia del expediente mencionado.

UNIDAD DE AUDITORIA INTERNA UNC FOLIO 25

SECRETARIA DE GESTION INSTITUCIONAL FOLIO

UNC U.A.I.	FECHA 13/12/16	DEPENDENCIA: SECRETARIA DE GESTION INSTITUCIONAL	PROYECTO DE AUDITORIA SISTEMAS INFORMÁTICOS SIU-DIAGUITA	OPINION DEL AUDITADO Y PLAN DE ACCION

HALLAZGOS		OPINION	PLAN DE ACCION		
Nº	DETALLE		FECHA INICIO	FECHA FINAL	DETALLE
5	5) No se ha de designado formalmente un responsable del monitoreo del registro de actividades o logs. con el fin de analizar periódicamente los logs, y documentar los resultados.	La Resol SPGI 159/2012 establece como Referentes Administrativos en sus artículos 11 y 15 a la Dirección General de Contrataciones en el caso del módulo compras y contrataciones y a la Dirección de Patrimonio y Rendición de Cuentas de la Dirección General de Contabilidad y Finanzas en el módulo patrimonio. En dichos artículos además se establece a la Dirección General de Tecnologías Informáticas (DGTI) como Referente Técnico del SIU Diaguita. Según los artículos 2 y 5 los referentes administrativos deben monitorear la adecuada registración de procesos y actividades y funcionamiento del sistema.			
6	6) No existe un procedimiento de registro y control de actividades de los usuarios respecto del uso del sistema.		marzo/17	Agosto/17	* Creación de un formulario para que el propietario de la información (referente administrativo) lo complete en conjunto con DGTI, el cual contendrá las especificaciones de registro y control de actividades de los usuarios respecto del uso del sistema. * Documentación y formalización del procedimiento.
7	7) No se realizan análisis periódicos de los logs de actividades.		marzo/17	Agosto/17	En base a las acciones a realizar del punto 6, se gestionará una herramienta para visualización de logs

UNIDAD DE AUDITORIA INTERNA UNC FOLIO 26

SECRETARIA DE GESTION INSTITUCIONAL FOLIO 44

UNC U.A.I.	FECHA 13/12/16	DEPENDENCIA: SECRETARIA DE GESTION INSTITUCIONAL	PROYECTO DE AUDITORIA SISTEMAS INFORMÁTICOS SIU-DIAGUITA	**OPINION DEL AUDITADO Y PLAN DE ACCION**

HALLAZGOS		OPINION	PLAN DE ACCION		
Nº	DETALLE		FECHA INICIO	FECHA FINAL	DETALLE
8	8) No existe un procedimiento formal definido y documentado para la puesta en producción del sistema o de nuevas versiones, asignando formalmente las responsabilidades para tal fin, con la verificación de la correcta implementación de los cambios, y diseñando los mecanismos necesarios, para que los técnicos y los usuarios, tomen conocimiento de los cambios que brinda el sistema ante la implementación de nuevas versiones.	El Sistema SIU Diaguita se encuentra en producción y su procedimiento de implementacion se encuentra documentado en Resol SPGI 174/2012 Y Resol.SPGI 131/2010. El procedimiento para el versionado del SIU Diaguita se coordina con los propietarios de la información (e_mail, etc)	marzo/17	Agosto/17	Documentación y formalización en conjunto con los referentes administrativos del procedimiento de versionado del SIU Diaguita
		FIRMA Y ACLARACION DEL RESPONSABLE DEL PLAN DE ACCION			FIRMA DEL DECANO, DIRECTOR O SECRETARIO

Esp. Ing. DIANA MASUERO
Directora de Operac. y Procesam. Informáticos
D.G.T.
Secretaría de Gestión Institucional

UNIVERSIDAD NACIONAL DE CORDOBA
Dirección Gral. de Tecnologías

Ing. LUCAS MANJARRÉS
Director de Equipamiento, Redes y Seg. Inf.
D G T
Secretaría de Gestión Institucional

UNC UNIDAD DE AUDITORIA INTERNA FOLIO 27

SECRETARÍA DE GESTIÓN INSTITUCIONAL FOLIO 98