Universidad Nacional de Moreno

Unidad de Auditoria Interna

Proyecto de Auditoría: Infraestructuras críticas de tecnología de información

Informe Nº: 13-2014

Tabla de Contenidos

Informe Ejecutivo

Informe Analítico

Informe Ejecutivo

I – Jurisdicción u Organismo y Titulo

Universidad Nacional de Moreno.

Proyecto de auditoría: Infraestructuras críticas de tecnología de información

Informe Nº 13-2014.

II – Síntesis - Conclusión

El presente Informe da cumplimiento al Plan de Auditoria 2014.

Su objetivo es evaluar el estado de situación del control interno las Infraestructuras críticas de tecnología de información de la Universidad Nacional de Moreno.

Las tareas fueron desarrolladas, a partir de un programa de trabajo específico emitido por la SIGEN, conforme el instructivo de trabajo N°3/2014 – GNyPE.

Las actividades de campo se llevaron a cabo entre el **20 de octubre** y el **17 de noviembre de 2014** 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:

Respecto al control interno de las Infraestructuras críticas de tecnología de información de la Universidad Nacional de Moreno, no se da cumplimiento a los ítems 3.3 Áreas Protegidas, 5.1 Registro de Visitas, 9.5 y 9.7 Seguridad física del CPD principal, 10.2 Mantenimiento de equipos, 13.1 Análisis de vulnerabilidades, del Instructivo de Trabajo N°3/2014 -GNyPE- Circular N° 1/2014, detallados en Anexo I.

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

Implementar mecanismos de control que permitan verificar el cumplimiento de la normativa vigente en materia de Tecnología de la Información.

Sobre la base de la tarea realizada, se concluye:

El estado de situación del control interno las Infraestructuras críticas de tecnología de información de la Universidad Nacional de Moreno, resulta razonable, excepto por los incumplimientos que se detallan en el apartado Observaciones del presente informe.

III – Lugar y fecha, firma y sello

Buenos Aires, noviembre de 2014.

Informe Analítico

Universidad Nacional de Moreno

Proyecto de Auditoría: Infraestructuras críticas de tecnología de información
Informe Nº 13-2014
Informe Analítico

I - Objeto

El presente Informe da cumplimiento al Plan de Auditoria 2014.

Su objetivo es evaluar el estado de situación del control interno las Infraestructuras críticas de tecnología de información de la Universidad Nacional de Moreno.

II - Alcance

Las tareas fueron desarrolladas, a partir de un programa de trabajo específico emitido por la SIGEN, conforme el instructivo de trabajo N°3/2014 – GNyPE.

Las actividades de campo se llevaron a cabo entre el **20 de octubre** y el **17 de noviembre de 2014** 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 el estado de situación del control interno de la tecnología informática de la Universidad, se aplicaron los siguientes procedimientos:

1. Relevar los puntos de control conforme el Instructivo de Trabajo N°3/2014 – GNyPE.

V – Marco de Referencia

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

- Instructivo de Trabajo N°3/2014 -GNyPE- Circular N° 1/2014.

VI – Circuito, tema o aspectos auditados

Ver anexo I.

VII – Observaciones

1. Respecto al control interno de las Infraestructuras críticas de tecnología de información de la Universidad Nacional de Moreno, no se da cumplimiento a los ítems 3.3 Áreas Protegidas, 5.1 Registro de Visitas, 9.5 y 9.7 Seguridad física del CPD principal, 10.2 Mantenimiento de equipos, 13.1 Análisis de vulnerabilidades, del Instructivo de Trabajo N°3/2014 -GNyPE- Circular N° 1/2014, detallados en Anexo I.

VIII – Recomendaciones

1. Implementar mecanismos de control que permitan verificar el cumplimiento de la normativa vigente en materia de Tecnología de la Información.

IX – Opinión del sector auditado

Ver anexo I.

X – Conclusión

El estado de situación del control interno las Infraestructuras críticas de tecnología de información de la Universidad Nacional de Moreno, resulta razonable, excepto por los incumplimientos que se detallan en el apartado Observaciones del presente informe.

XI – Lugar y fecha, firma y sello

Buenos Aires, noviembre de 2014.

Anexo I.

Instructivo de Trabajo Nº 3/2014 - GNyPE

Infraestructuras Críticas De Tecnología De Información

Aspectos descriptivos
1. El CPD (Centro de Procesamiento de Datos) donde se alojan los servicios informáticos críticos del organismo, es administrado por: el Organismo 2. Los servidores/equipos donde residen los servicios informáticos críticos del Organismo, se encuentran ubicados en: CPD Principal, en el Organismo 3. Especifique el proveedor de energía contratado para los servicios informáticos críticos del Organismo: CPD Principal: Indicar nombre, hasta 3: EDENOR 4. Especifique el proveedor de enlaces de telecomunicaciones para los servicios informáticos críticos del Organismo: CPD Principal: Indicar nombre, hasta 3: RIU JFX 5. Indicar la ventana de tiempo en que el Organismo puede operar sin que funcionen los servicios críticos de TI: Se tolera interrupción. Indicar lapso de tolerancia: 6 hs. 6. Ante una contingencia que pudiera afectar el normal procesamiento de las operaciones en el CPD Principal, ¿el Organismo cuenta con un Sitio de Procesamiento Alternativo? No, en construcción

Aspectos Generales de Control

1. POLÍTICA DE SEGURIDAD					
	Cumple				
Aspecto a verificar	sí	no	Parcial	N/A	Comentarios
1.1. ¿Se posee una política de seguridad de la información?	x				
1.1.1. ¿La política se encuentra aprobada?			x		
1.1.2. ¿La política responde a lo requerido por la Disposición 3/2013, Política de Seguridad de la Información Modelo,			x		

publicada en el B.O. 27/8/2013?					
1.1.3. La Política de Seguridad u otro documento formal ¿identifica claramente cuáles son los elementos de infraestructura que resultan críticos para el funcionamiento de la tecnología informática de la organización?	x				
2. RESPONSABILIDAD POR LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS					
	Cumple				
Aspecto a verificar	sí	no	Parcial	N/A	Comentarios
2.1. ¿Se ha asignado formalmente la responsabilidad por la protección de las infraestructuras críticas de información?	x				
3. CONTROLES DE ACCESO AL CPD- ÁREAS PROTEGIDAS					
	Cumple				
Aspecto a verificar	sí	no	Parcial	N/A	Comentarios
3.1. ¿El responsable de Seguridad lleva un registro de los sitios protegidos que al menos indique los siguientes ítems?: - identificación del edificio y área - principales elementos a proteger - medidas de protección física.	x				
3.2. ¿El CPD Principal se encuentra ubicado en un lugar al cual no pueda acceder el personal no autorizado?	x				
3.3. ¿Se lleva un registro de las visitas a áreas protegidas?		x			
3.4. ¿Se lleva un registro actualizado de las personas autorizadas a acceder a las áreas protegidas?	x				en implementación
3.5. ¿Se revisan y actualizan con frecuencia los derechos de acceso a las áreas protegidas?	x				en implementación
4. CONTROLES DE ACCESO AL CPD- PROTECCIÓN FÍSICA DE ACCESOS					
	Cumple				
Aspecto a verificar	sí	no	Parcial	N/A	Comentarios
4.1. ¿Existen controles asociados a la protección física de accesos al CPD?	x				
5. CONTROLES DE ACCESO AL CPD-REGISTRO DE VISITAS					
	Cumple				
Aspecto a verificar	sí	no	Parcial	N/A	Comentarios
5.1. ¿Existen controles asociados al registro de visitas al CPD?		x			
5.1.1. ¿El acceso del personal del servicio de soporte externo al CPD Principal, es debidamente registrado, autorizado, otorgado y monitoreado?			x		
6. INSTALACIONES DE SUMINISTRO DE ENERGÍA DEL CPD PRINCIPAL					
	Cumple				
Aspecto a verificar	sí	no	Parcial	N/A	Comentarios
6.1. ¿El equipamiento está protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas?	x				

6.2. ¿El suministro de energía, cumple con las especificaciones del fabricante o proveedor de cada equipo?	x				
6.3. ¿Se dispone de múltiples líneas de suministro para evitar un único punto de falla en el suministro de energía?	x				
7. SUMINISTRO DE ENERGÍA INTERRUMPIBLE (UPS) DEL CPD PRINCIPAL					
	Cumple				
Aspecto a verificar	sí	no	Parcial	N/A	Comentarios
7.1. ¿Se cuenta con un suministro de energía interrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas en el CPD Principal del Organismo?	x				
7.1.1. ¿Los equipos de UPS son inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida?	x				
8.GENERADOR DE RESPALDO DEL CPD Principal					
	Cumple				
Aspecto a verificar	sí	no	Parcial	N/A	Comentarios
8.1. ¿Se dispone de un generador de respaldo (y su correspondiente suministro de combustible) para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía en el CPD Principal?	x				
8.1.1. ¿ Los generadores de respaldo son inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen autonomía requerida?	x				
9. SEGURIDAD FÍSICA DEL CPD PRINCIPAL					
	Cumple				
Aspecto a verificar	sí	no	Parcial	N/A	Comentarios
9.1. ¿Se cumple con los requisitos técnicos vigentes de la República Argentina?			x		
9.2. ¿Se utiliza piso ducto o cableado embutido en la pared en el CPD Principal?	x				
9.3. ¿Los cables de energía están separados de los cables de comunicaciones para evitar interferencias?	x				
9.4. ¿El CPD Principal cuenta con aire acondicionado principal y de respaldo?			x		
9.5. ¿El CPD Principal cuenta con alarmas por alta temperatura?		x			
9.6. ¿El CPD Principal cuenta con extinguidores automáticos y/o manuales?	x				
9.7. ¿El CPD Principal cuenta con detectores de humo y humedad?		x			
9.8. ¿Los materiales peligrosos o combustibles se encuentran a una distancia prudencial de las áreas protegidas del Organismo?			x		
10. MANTENIMIENTO DE LOS EQUIPOS CRÍTICO					
	Cumple				
Aspecto a verificar	sí	no	Parcial	N/A	Comentarios

10.1 ¿El área de Informática mantiene un listado actualizado del equipamiento crítico con el detalle de la frecuencia en que se realizará el mantenimiento preventivo, los retiros para mantenimiento, etc.?			x		
10.2.¿ Se registran todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado?			x		
10.3. ¿Se registran los equipos críticos que se retiran para mantenimiento, previa eliminación de información confidencial y copias de resguardo?				x	
11.RESPALDO O BACK-UP					
	Cumple				
Aspecto a verificar	sí	no	Parcial	N/A	Comentarios
11.1. ¿Los sistemas críticos se encuentran identificados?	x				
11.2. ¿Se cuenta con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico del Organismo?	x				
11.3. ¿El procedimiento de resguardo de la información crítica se encuentra formalmente documentado y aprobado?			x		
11.4. ¿El responsable del área informática dispone y controla la realización de las copias de resguardo críticas, así como la prueba periódica de su restauración e integridad?	x				
11.5. ¿Se almacenan copias de resguardo en otra ubicación diferente al CPD Principal, en un sito alejado del mismo?	x				
12. GESTIÓN DE INCIDENTES					
	Cumple				
Aspecto a verificar	sí	no	Parcial	N/A	Comentarios
12.1. ¿Existe un procedimiento formal de comunicación y de respuesta a incidentes de seguridad de TI en el CPD Principal?			x		
12.2. ¿Los incidentes de seguridad son comunicados a través de las autoridades o canales apropiados tan pronto como sea posible?	x				
12.3. ¿El responsable de Seguridad de la información es informado tan pronto como se haya tomado conocimiento de cualquier incidente o violación de seguridad?	x				
12.4. ¿Han adherido al "Programa Nacional de Infraestructura Críticas de Información y Ciberseguridad" (ICIC), según lo aprobado por la Disposición N° 3/2011 ONTI?	x				
13. ANÁLISIS DE VULNERABILIDADES					
	Cumple				
Aspecto a verificar	sí	no	Parcial	N/A	Comentarios
13.1. ¿Se realizan escaneos de vulnerabilidades en los servidores alojados en el CPD Principal?		x			
13.1.1. En caso de detectar vulnerabilidades, ¿se toman las medidas necesarias para tratar los riesgos asociados?	x				
14. GESTIÓN DE CONTINGENCIAS					
	Cumple				
Aspecto a verificar	sí	no	Parcial	N/A	Comentarios

14.1. Ante la ocurrencia de una contingencia que comprometa la disponibilidad del CPD, ¿el Organismo cuenta con un Plan de Contingencia o Plan de recuperación ante Desastres?			x		
14.1.1. ¿El Plan de Contingencia o Plan de Recuperación ante Desastres se encuentra documentado, probado y aprobado?			x		
14.1.2. ¿Se han definido los sistemas críticos y su prioridad de recuperación?			x		
14.1.3. ¿Se encuentran formalmente acordados los tiempos de recuperación para los servicios críticos?		x			
14.1.4. ¿Se han definido claramente los roles y responsabilidades de los equipos de trabajos encargados de la recuperación de los sistemas críticos?	x				
14.1.5. ¿Se han documentado detalladamente los procedimientos técnicos para restaurar cada uno de los sistemas críticos?			x		