# Universidad Nacional de Moreno

## Unidad de Auditoria Interna

## Proyecto de Auditoría: Tecnología de la Información
## Sistemas Informáticos y bases de datos críticas

## Informe Nº: 13-2017

Tabla de Contenidos

## Informe Ejecutivo



## Informe Analítico

# Informe Ejecutivo

## I – Jurisdicción u Organismo y Titulo

Universidad Nacional de Moreno.

Proyecto de auditoría: Tecnología de la Información. Sistemas informáticos y bases de datos críticas.

Informe Nº 13-2017.

## II – Síntesis - Conclusión

El presente Informe da cumplimiento al Plan de Auditoria 2017.

Su objetivo es verificar los controles asociados a sistemas informáticos y bases de datos críticas, 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°3/2017 – SLyT.

Las actividades de campo se llevaron a cabo entre el **3 de julio** y el **31 de agosto** del corriente, 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:
No hay observaciones que informar.

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

No hay recomendaciones que realizar.

Sobre la base de la tarea realizada, se concluye:

Los controles internos asociados a los sistemas informáticos y bases de datos críticas, que utiliza la Universidad Nacional de Moreno, resultan razonables en sus aspectos significativos, respecto de los controles mencionados en el Instructivo de Trabajo Nº 3/2017 – SLyT.

## III – Lugar y fecha, firma y sello

**Buenos Aires,** 31 de agosto de 2017.

# Informe Analítico

**Universidad Nacional de Moreno**

# Proyecto de Auditoría: Tecnología de la Información.
# Sistemas informáticos y bases de datos críticas.
# Informe Nº 13-2017

## Informe Analítico

### I - Objeto

El presente Informe da cumplimiento al Plan de Auditoria 2017.

Su objetivo es verificar los controles asociados a sistemas informáticos y bases de datos críticas, 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°3/2017 – SLyT.

Las actividades de campo se llevaron a cabo entre el **3 de julio** y el **31 de agosto** del corriente, 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 los controles asociados a sistemas informáticos y bases de datos críticas de la Universidad, se aplicaron los siguientes procedimientos:

1. Relevar los puntos de control conforme el Instructivo de Trabajo N°3/2017 – SLyT.

### V – Marco de Referencia

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

- Instructivo de Trabajo N°3/2017 – SLyT.

## VI – Circuito, tema o aspectos auditados

Conforme el Instructivo de trabajo, se relevó la siguiente información:

| **Datos descriptivos** | |
|---|---|
| **1.1. Nombre del Sistema:** | **SIU-Pilaga** |
| **1.2. Descripción:** | Gestión presupuestaria, financiera y contable |
| **1.3. Procesos críticos soportados por el Sistema (incluir hasta 5, solo los principales):** | |
| **1.4. Lenguaje / Tecnología de Desarrollo:** | |
| Visual Basic | |
| Ruby | |
| PHP | si |
| Java | |
| Cobol | |
| Delphi | |
| Python | |
| ASP.NET | |
| ASP | |
| VB.NET | |
| C | |
| C++ | |
| C# | |
| Perl | |
| Otros: | |
| **1.7. Cantidad de tablas de la Base de Datos:** | 528 |
| **1.8. Crecimiento mensual promedio aproximado en tamaño (en %):** | 3% |
| **1.9. La Base de Datos ¿tiene información de personas? (Habeas Data):** | NO |
| **1.10. La Base de Datos:** | |
| No maneja datos económicos/financieros | SI |
| Administra datos por montos económicos menores a $100 millones anuales | |
| Administra datos por valores económicos entre $100 y $1.000 millones anuales | |
| Administra datos por valores económicos entre $1.000 y $10.000 millones anuales | |
| Administra datos por más de $10.000 millones anuales | SI |
| **1.11. Ubicación de la Base de Datos:** | |
| En ubicaciones del Organismo | SI |
| En instalaciones de un proveedor en Argentina | |
| En instalaciones de un proveedor fuera de Argentina | |
| Otros Organismos del Sector Público Nacional: | |
| **1.12. Cantidad aproximada de Usuarios que utilizan el Sistema:** | |

| | |
|---|---|
| - Usuarios internos: | 38 |
| - Usuarios externos: | No posee |
| Ciudadanos (indicar cant. aprox.): | No posee |
| Otros Organismos públicos (indicar cant. aprox.): | No posee |
| En este caso indicar nombre/denominación del/los Organismo/s: | - |
| Otros (ej. Empresas. Indicar cant. aprox.): | - |
| **1.13. Criticidad del sistema. "Ventana de tiempo" en que la organización puede operar sin que el Sistema funcione:** | |
| Sistema de alta criticidad. Se requiere operación 24*365 | |
| Se tolera interrupción de hasta 24 horas | |
| La ventana de disponibilidad es de más de 24 horas: indicar lapso de tolerancia | 3 días |
| **1.14. Antigüedad del Sistema (en años)** | |
| Menor a 1 año | |
| Entre 1 y 5 años | |
| Mayor a 5 años | X |
| **1.15. Origen del Sistema:** | |
| Desarrollo interno en el Organismo | |
| Desarrollo interno a medida realizado por terceros | |
| Otros organismos del Sector Público Nacional | SIU (Sistemas de información Universitario) |
| Sistema enlatado ( Indicar nombre del Proveedor) | |

## 2. CONTROL INTERNO

| **2.1. Información Base de datos:** | | | | |
|---|---|---|---|---|
| | **Cumple** | | | **Comentarios** |
| **Aspecto a Verificar** | **Sí** | **No** | **Parcialmente** | |
| 2.1.1. ¿Se ha clasificado la información administrada por el Sistema según su nivel de criticidad, considerando lo expuesto en la Política de Seguridad Modelo aprobada mediante Disp. N°1/2015 ONTI (Cláusula 8 – Gestión de Activos)? | X | | | |
| 2.1.2. El Sistema, ¿permite generar información ejecutiva, ágil y oportuna para la toma de decisiones por parte de la conducción? | X | | | |
| 2.1.3. Los datos del Sistema ¿resultan confiables para los usuarios destinatarios de la información? | X | | | |
| 2.1.4. ¿Se realizan cruzamientos periódicos de datos con otras bases de datos del Organismo o de otros Organismos? (por ejemplo: Datos de personas contra fallecidos, RENAPER, datos de ANSES, datos de AFIP, etc.) | X | | | |
| **2.2. Documentación Técnica del Sistema:** | | | | |
| 2.2.1. ¿Se dispone de documentación de los aspectos técnicos del Sistema? | X | | | |
| 2.2.2. La documentación técnica ¿es completa y se encuentra actualizada? | | | Existe documentación básica suministrada por el proveedor del | |

| | | | | |
|---|---|---|---|---|
| | | | sistema | |
| **2.3. Manual de Usuario del Sistema:** | | | | |
| 2.3.1. ¿Se dispone de Manual del Usuario? | X | | | Existen manuales en línea |
| 2.3.2. El Manual de Usuario ¿se encuentra actualizado y disponible/accesible para todos los usuarios? | | | | Se pueden acceder a través de intranet de la institución Son mantenidos por el proveedor del sistema (SIU) |
| **2.4. Cambios a programas:** | | | | |
| 2.4.1. ¿Existen procedimientos definidos para la puesta en producción del sistema o nuevas versiones? | X | | | |
| 2.4.2. ¿Se han asignado formalmente las responsabilidades para la realización de pruebas, puesta en producción de nuevas versiones del sistema y su configuración? | X | | | |
| 2.4.3. ¿Se dispone de un registro de versiones y cambios a programas? | X | | | No se realiza desarrollo sobre los mismos, solo cambios de versión |
| 2.4.4. ¿Se verifica la correcta implementación de los cambios? | x | | | Para cambios de versión |
| 2.4.5. ¿Se lleva a cabo una aprobación formal de los cambios que se efectúan, por parte de las áreas propietarias del sistema y del área de TI? | x | | | Para cambios de versión |
| **2.5. Permisos de acceso al Sistema:** | | | | |
| 2.5.1. El acceso al sistema ¿se realiza mediante permisos de acceso? | X | | | |
| 2.5.2. El procedimiento de gestión de permisos ¿se encuentra documentado? | | | X | |
| 2.5.3. ¿Se utilizan identificadores de usuario únicos (es decir por persona, no genéricos)? | X | | | |
| 2.5.4. ¿Se realizan controles periódicos sobre los permisos de usuarios vigentes a fin de realizar las modificaciones necesarias, y de cancelar identificadores y cuentas de usuario redundantes o inactivas? | X | | | Semestralmente. |
| 2.5.5. ¿Se requirió a los usuarios que suscriban una declaración por la cual se comprometen a no difundir su contraseña de acceso al sistema? | | X | | Se encuentra en estudio del área un mecanismo institucional que permita obtener el compromiso firmado de los usuarios al debido uso del, equipamiento, aplicativos, datos y claves de acceso. |
| **2.6. Logs o Registros de Transacciones del Sistema:** | | | | |
| 2.6.1. ¿Se mantienen logs o registros de uso para las funciones críticas del sistema? | X | | | |
| 2.6.2. ¿Existe un procedimiento documentado para el resguardo y análisis de los logs? | X | | | Todos sistemas de SIU resguardan su log en la base de datos, y el |

| | | | | |
|---|---|---|---|---|
| | | | | backup se realiza en ese contexto |
| 2.6.3. ¿Se mantienen backups de los logs críticos por un período razonable? | X | | | |
| **2.7. Acceso a datos:** | | | | |
| 2.7.1. ¿Se restringe apropiadamente el acceso directo a los datos por fuera de las funciones del sistema? | X | | | Ningún usuario tiene acceso a los datos por fuera de los sistemas. Únicamente el personal de desarrollo de la STIC, puede acceder a los datos, dependiendo del grado de responsabilidad que tenga en la implementación de cada sistema. No es posible restringir esto los desarrolladores porque no habría posibilidad de administrar los sistemas. |
| 2.7.2. ¿Se mantiene un log de accesos a los datos críticos de la base de datos o archivos? | | | X | Se mantiene este registro para los usuarios finales; no así para los accesos por parte de los administradores |
| **2.8. Backup del Sistema:** | | | | |
| 2.8.1. ¿Se realizan backups periódicos de los datos, programas y configuración del sistema? | X | | | |
| 2.8.2. ¿Existe un procedimiento documentado para la realización de backups del sistema? | | | X | Se está trabajando en la documentación formal del backup |
| 2.8.3. Los backups ¿se almacenan en un sitio con acceso restringido y suficientes medidas de seguridad? | X | | | |
| 2.8.4. ¿Se mantiene un backup periódico en un sitio externo? | X | | | |
| 2.8.5. ¿Se prueban los backups y su recuperación en forma periódica, para garantizar que cumplen con los requerimientos de los planes de continuidad de las actividades? | X | | | |
| **2.9. Preparación para recuperación ante contingencia:** | | | | |
| 2.9.1. ¿Se dispone de procedimientos documentados y aprobados para la recuperación del sistema ante fallas o contingencias? | | | | |
| 2.9.2. ¿Se realizan pruebas de recuperación periódicas? | X | | | |
| 2.9.3. ¿Se han definido claramente los roles y responsabilidades del equipo de trabajo encargado de la recuperación del sistema? | | X | | |
| **2.10. Análisis UAI:** | | | | |

| | | | | |
|---|---|---|---|---|
| 2.10.1. La UAI ¿ha realizado en los últimos 2 años un análisis sobre la calidad de los datos del sistema utilizando herramientas de TI a tal fin? (es decir, validar si los datos responden a los formatos y controles de los campos, verificar la presencia de inconsistencias, datos en blanco, etc.) (Nota: en caso afirmativo, indicar en Comentarios los informes que reflejan los resultados obtenidos) | X | | | |

| **Datos descriptivos** | |
|---|---|
| **1.1. Nombre del Sistema:** | **SIU-MAPUCHE** |
| **1.2. Descripción:** | Gestión de Recursos Humanos |
| **1.3. Procesos críticos soportados por el Sistema (incluir hasta 5, solo los principales):** | |
| **1.4. Lenguaje / Tecnología de Desarrollo:** | |
| Visual Basic | |
| Ruby | |
| PHP | si |
| Java | |
| Cobol | |
| Delphi | |
| Python | |
| ASP.NET | |
| ASP | |
| VB.NET | |
| C | |
| C++ | |
| C# | |
| Perl | |
| Otros: | |
| **1.7. Cantidad de tablas de la Base de Datos:** | 446 |
| **1.8. Crecimiento mensual promedio aproximado en tamaño (en %):** | 5% |
| **1.9. La Base de Datos ¿tiene información de personas? (Habeas Data):** | SI |
| **1.10. La Base de Datos:** | |
| No maneja datos económicos/financieros | SI |
| Administra datos por montos económicos menores a $100 millones anuales | |
| Administra datos por valores económicos entre $100 y $1.000 millones anuales | |
| Administra datos por valores económicos entre $1.000 y $10.000 millones anuales | |
| Administra datos por más de $10.000 millones anuales | SI |
| **1.11. Ubicación de la Base de Datos:** | |
| En ubicaciones del Organismo | SI |
| En instalaciones de un proveedor en Argentina | |
| En instalaciones de un proveedor fuera de Argentina | |
| Otros Organismos del Sector Público Nacional: | |
| **1.12. Cantidad aproximada de Usuarios que utilizan el Sistema:** | |
| - Usuarios internos: | 24 |

| | |
|---|---|
| - Usuarios externos: | No posee |
| Ciudadanos (indicar cant. aprox.): | - |
| Otros Organismos públicos (indicar cant. aprox.): | - |
| En este caso indicar nombre/denominación del/los Organismo/s: | - |
| Otros (ej. Empresas. Indicar cant. aprox.): | - |
| **1.13. Criticidad del sistema. "Ventana de tiempo" en que la organización puede operar sin que el Sistema funcione:** | |
| Sistema de alta criticidad. Se requiere operación 24*365 | |
| Se tolera interrupción de hasta 24 horas | |
| La ventana de disponibilidad es de más de 24 horas: indicar lapso de tolerancia | 3 días |
| **1.14. Antigüedad del Sistema (en años)** | |
| Menor a 1 año | |
| Entre 1 y 5 años | X |
| Mayor a 5 años | |
| **1.15. Origen del Sistema:** | |
| Desarrollo interno en el Organismo | |
| Desarrollo interno a medida realizado por terceros | |
| Otros organismos del Sector Público Nacional | SIU (Sistemas de información Universitario) |
| Sistema enlatado ( Indicar nombre del Proveedor) | |

## 2. CONTROL INTERNO

| **2.1. Información Base de datos:** | | | | |
|---|---|---|---|---|
| | **Cumple** | | | **Comentarios** |
| **Aspecto a Verificar** | **Sí** | **No** | **Parcialmente** | |
| 2.1.1. ¿Se ha clasificado la información administrada por el Sistema según su nivel de criticidad, considerando lo expuesto en la Política de Seguridad Modelo aprobada mediante Disp. N°1/2015 ONTI (Cláusula 8 – Gestión de Activos)? | X | | | |
| 2.1.2. El Sistema, ¿permite generar información ejecutiva, ágil y oportuna para la toma de decisiones por parte de la conducción? | X | | | |
| 2.1.3. Los datos del Sistema ¿resultan confiables para los usuarios destinatarios de la información? | X | | | |
| 2.1.4. ¿Se realizan cruzamientos periódicos de datos con otras bases de datos del Organismo o de otros Organismos? (por ejemplo: Datos de personas contra fallecidos, RENAPER, datos de ANSES, datos de AFIP, etc.) | X | | | |
| **2.2. Documentación Técnica del Sistema:** | | | | |
| 2.2.1. ¿Se dispone de documentación de los aspectos técnicos del Sistema? | X | | | |
| 2.2.2. La documentación técnica ¿es completa y se encuentra actualizada? | | | Existe documentación básica suministrada por el proveedor del sistema | |
| **2.3. Manual de Usuario del Sistema:** | | | | |
| 2.3.1. ¿Se dispone de Manual del Usuario? | X | | | Existen |

| | | | | |
|---|---|---|---|---|
| | | | | manuales en línea |
| 2.3.2. El Manual de Usuario ¿se encuentra actualizado y disponible/accesible para todos los usuarios? | | | | Se pueden acceder a través de intranet de la institución Son mantenidos por el proveedor del sistema (SIU) |
| **2.4. Cambios a programas:** | | | | |
| 2.4.1. ¿Existen procedimientos definidos para la puesta en producción del sistema o nuevas versiones? | X | | | |
| 2.4.2. ¿Se han asignado formalmente las responsabilidades para la realización de pruebas, puesta en producción de nuevas versiones del sistema y su configuración? | X | | | |
| 2.4.3. ¿Se dispone de un registro de versiones y cambios a programas? | X | | | No se realiza desarrollo sobre los mismos, solo cambios de versión |
| 2.4.4. ¿Se verifica la correcta implementación de los cambios? | X | | | Para cambios de versión |
| 2.4.5. ¿Se lleva a cabo una aprobación formal de los cambios que se efectúan, por parte de las áreas propietarias del sistema y del área de TI? | X | | | Para cambios de versión |
| **2.5. Permisos de acceso al Sistema:** | X | | | |
| 2.5.1. El acceso al sistema ¿se realiza mediante permisos de acceso? | X | | | |
| 2.5.2. El procedimiento de gestión de permisos ¿se encuentra documentado? | | | X | |
| 2.5.3. ¿Se utilizan identificadores de usuario únicos (es decir por persona, no genéricos)? | X | | | |
| 2.5.4. ¿Se realizan controles periódicos sobre los permisos de usuarios vigentes a fin de realizar las modificaciones necesarias, y de cancelar identificadores y cuentas de usuario redundantes o inactivas? | X | | | Semestralmente . |
| 2.5.5. ¿Se requirió a los usuarios que suscriban una declaración por la cual se comprometen a no difundir su contraseña de acceso al sistema? | | X | | Se encuentra en estudio del área un mecanismo institucional que permita obtener el compromiso firmado de los usuarios al debido uso del, equipamiento, aplicativos, datos y claves de acceso. |
| **2.6. Logs o Registros de Transacciones del Sistema:** | | | | |
| 2.6.1. ¿Se mantienen logs o registros de uso para las funciones críticas del sistema? | X | | | |
| 2.6.2. ¿Existe un procedimiento documentado para el resguardo y análisis de los logs? | X | | | Todos sistemas de SIU resguardan su log en la base de datos, y el backup se realiza en ese contexto |
| 2.6.3. ¿Se mantienen backups de los logs críticos por un período razonable? | X | | | |

| | | | | |
|---|---|---|---|---|
| **2.7. Acceso a datos:** | | | | |
| 2.7.1. ¿Se restringe apropiadamente el acceso directo a los datos por fuera de las funciones del sistema? | X | | | Ningún usuario tiene acceso a los datos por fuera de los sistemas. Únicamente el personal de desarrollo de la STIC, puede acceder a los datos, dependiendo del grado de responsabilidad que tenga en la implementación de cada sistema. No es posible restringir esto los desarrolladores porque no habría posibilidad de administrar los sistemas. |
| 2.7.2. ¿Se mantiene un log de accesos a los datos críticos de la base de datos o archivos? | | | X | Se mantiene este registro para los usuarios finales; no así para los accesos por parte de los administradores |
| **2.8. Backup del Sistema:** | | | | |
| 2.8.1. ¿Se realizan backups periódicos de los datos, programas y configuración del sistema? | X | | | |
| 2.8.2. ¿Existe un procedimiento documentado para la realización de backups del sistema? | | | X | Se está trabajando en la documentación formal del backup |
| 2.8.3. Los backups ¿se almacenan en un sitio con acceso restringido y suficientes medidas de seguridad? | X | | | |
| 2.8.4. ¿Se mantiene un backup periódico en un sitio externo? | X | | | |
| 2.8.5. ¿Se prueban los backups y su recuperación en forma periódica, para garantizar que cumplen con los requerimientos de los planes de continuidad de las actividades? | X | | | |
| **2.9. Preparación para recuperación ante contingencia:** | | | | |
| 2.9.1. ¿Se dispone de procedimientos documentados y aprobados para la recuperación del sistema ante fallas o contingencias? | | | | |
| 2.9.2. ¿Se realizan pruebas de recuperación periódicas? | X | | | |
| 2.9.3. ¿Se han definido claramente los roles y responsabilidades del equipo de trabajo encargado de la recuperación del sistema? | | X | | |
| **2.10. Análisis UAI:** | | | | |

| | | | | |
|---|---|---|---|---|
| 2.10.1. La UAI ¿ha realizado en los últimos 2 años un análisis sobre la calidad de los datos del sistema utilizando herramientas de TI a tal fin? (es decir, validar si los datos responden a los formatos y controles de los campos, verificar la presencia de inconsistencias, datos en blanco, etc.) (Nota: en caso afirmativo, indicar en Comentarios los informes que reflejan los resultados obtenidos) | | | | |

| **Datos descriptivos** | |
|---|---|
| **1.1. Nombre del Sistema:** | **SIU-GUARANI** |
| **1.2. Descripción:** | Registra y administra las actividades académicas de la universidad, desde que los alumnos ingresan como aspirantes hasta que obtienen el diploma |
| **1.3. Procesos críticos soportados por el Sistema (incluir hasta 5, solo los principales):** | |
| **1.4. Lenguaje / Tecnología de Desarrollo:** | |
| Visual Basic | |
| Ruby | |
| PHP | si |
| Java | |
| Cobol | |
| Delphi | |
| Python | |
| ASP.NET | |
| ASP | |
| VB.NET | |
| C | |
| C++ | |
| C# | |
| Perl | |
| Otros: | |
| | |
| **1.7. Cantidad de tablas de la Base de Datos:** | 593 |
| **1.8. Crecimiento mensual promedio aproximado en tamaño (en %):** | 6% |
| **1.9. La Base de Datos ¿tiene información de personas? (Habeas Data):** | SI |
| **1.10. La Base de Datos:** | |
| No maneja datos económicos/financieros | NO |
| Administra datos por montos económicos menores a $100 millones anuales | |
| Administra datos por valores económicos entre $100 y $1.000 millones anuales | |
| Administra datos por valores económicos entre $1.000 y $10.000 millones anuales | |
| Administra datos por más de $10.000 millones anuales | |
| **1.11. Ubicación de la Base de Datos:** | |
| En ubicaciones del Organismo | SI |
| En instalaciones de un proveedor en Argentina | |

| | |
|---|---|
| En instalaciones de un proveedor fuera de Argentina | |
| Otros Organismos del Sector Público Nacional: | |
| **1.12. Cantidad aproximada de Usuarios que utilizan el Sistema:** | |
| - Usuarios internos: | 100 |
| - Usuarios externos: | 18373 |
| Ciudadanos (indicar cant. aprox.): | - |
| Otros Organismos públicos (indicar cant. aprox.): | - |
| En este caso indicar nombre/denominación del/los Organismo/s: | - |
| Otros (ej. Empresas. Indicar cant. aprox.): | - |
| **1.13. Criticidad del sistema. "Ventana de tiempo" en que la organización puede operar sin que el Sistema funcione:** | |
| Sistema de alta criticidad. Se requiere operación 24*365 | |
| Se tolera interrupción de hasta 24 horas | |
| La ventana de disponibilidad es de más de 24 horas: indicar lapso de tolerancia | 3 días |
| **1.14. Antigüedad del Sistema (en años)** | |
| Menor a 1 año | |
| Entre 1 y 5 años | X |
| Mayor a 5 años | |
| **1.15. Origen del Sistema:** | |
| Desarrollo interno en el Organismo | |
| Desarrollo interno a medida realizado por terceros | |
| Otros organismos del Sector Público Nacional | SIU (Sistemas de información Universitario) |
| Sistema enlatado ( Indicar nombre del Proveedor) | |

## 2. CONTROL INTERNO

| **2.1. Información Base de datos:** | | | | |
|---|---|---|---|---|
| | **Cumple** | | | **Comentarios** |
| **Aspecto a Verificar** | **Sí** | **No** | **Parcialmente** | |
| 2.1.1. ¿Se ha clasificado la información administrada por el Sistema según su nivel de criticidad, considerando lo expuesto en la Política de Seguridad Modelo aprobada mediante Disp. N°1/2015 ONTI (Cláusula 8 – Gestión de Activos)? | | | | |
| 2.1.2. El Sistema, ¿permite generar información ejecutiva, ágil y oportuna para la toma de decisiones por parte de la conducción? | X | | | |
| 2.1.3. Los datos del Sistema ¿resultan confiables para los usuarios destinatarios de la información? | X | | | |
| 2.1.4. ¿Se realizan cruzamientos periódicos de datos con otras bases de datos del Organismo o de otros Organismos? (por ejemplo: Datos de personas contra fallecidos, RENAPER, datos de ANSES, datos de AFIP, etc.) | X | | | |
| **2.2. Documentación Técnica del Sistema:** | | | | |
| 2.2.1. ¿Se dispone de documentación de los aspectos técnicos del Sistema? | X | | | |
| 2.2.2. La documentación técnica ¿es completa y se encuentra actualizada? | | | Existe documentación básica | |

| | | | | |
|---|---|---|---|---|
| | | | suministrada por el proveedor del sistema | |
| **2.3. Manual de Usuario del Sistema:** | | | | |
| 2.3.1. ¿Se dispone de Manual del Usuario? | X | | | Existen manuales en línea |
| 2.3.2. El Manual de Usuario ¿se encuentra actualizado y disponible/accesible para todos los usuarios? | X | | | Se pueden acceder a través de intranet de la institución Son mantenidos por el proveedor del sistema (SIU) |
| **2.4. Cambios a programas:** | | | | |
| 2.4.1. ¿Existen procedimientos definidos para la puesta en producción del sistema o nuevas versiones? | X | | | |
| 2.4.2. ¿Se han asignado formalmente las responsabilidades para la realización de pruebas, puesta en producción de nuevas versiones del sistema y su configuración? | X | | | |
| 2.4.3. ¿Se dispone de un registro de versiones y cambios a programas? | X | | | |
| 2.4.4. ¿Se verifica la correcta implementación de los cambios? | X | | | |
| 2.4.5. ¿Se lleva a cabo una aprobación formal de los cambios que se efectúan, por parte de las áreas propietarias del sistema y del área de TI? | X | | | |
| **2.5. Permisos de acceso al Sistema:** | | | | |
| 2.5.1. El acceso al sistema ¿se realiza mediante permisos de acceso? | X | | | |
| 2.5.2. El procedimiento de gestión de permisos ¿se encuentra documentado? | | | X | |
| 2.5.3. ¿Se utilizan identificadores de usuario únicos (es decir por persona, no genéricos)? | X | | | |
| 2.5.4. ¿Se realizan controles periódicos sobre los permisos de usuarios vigentes a fin de realizar las modificaciones necesarias, y de cancelar identificadores y cuentas de usuario redundantes o inactivas? | X | | | Semestralmente . |
| 2.5.5. ¿Se requirió a los usuarios que suscriban una declaración por la cual se comprometen a no difundir su contraseña de acceso al sistema? | | X | | Se encuentra en estudio del área un mecanismo institucional que permita obtener el compromiso firmado de los usuarios al debido uso del, equipamiento, aplicativos, datos y claves de acceso. |
| **2.6. Logs o Registros de Transacciones del Sistema:** | | | | |
| 2.6.1. ¿Se mantienen logs o registros de uso para las funciones críticas del sistema? | X | | | |
| 2.6.2. ¿Existe un procedimiento documentado para el resguardo y análisis de los logs? | X | | | Todos sistemas de SIU resguardan su log en la base de datos, y el backup se realiza en ese |

| | | | | |
|---|---|---|---|---|
| | | | | contexto |
| 2.6.3. ¿Se mantienen backups de los logs críticos por un período razonable? | X | | | |
| **2.7. Acceso a datos:** | | | | |
| 2.7.1. ¿Se restringe apropiadamente el acceso directo a los datos por fuera de las funciones del sistema? | X | | | Ningún usuario tiene acceso a los datos por fuera de los sistemas. Únicamente el personal de desarrollo de la STIC, puede acceder a los datos, dependiendo del grado de responsabilidad que tenga en la implementación de cada sistema. No es posible restringir esto los desarrolladores porque no habría posibilidad de administrar los sistemas. |
| 2.7.2. ¿Se mantiene un log de accesos a los datos críticos de la base de datos o archivos? | | | X | Se mantiene este registro para los usuarios finales; no así para los accesos por parte de los administradores |
| **2.8. Backup del Sistema:** | | | | |
| 2.8.1. ¿Se realizan backups periódicos de los datos, programas y configuración del sistema? | X | | | |
| 2.8.2. ¿Existe un procedimiento documentado para la realización de backups del sistema? | | | X | Se está trabajando en la documentación formal del backup |
| 2.8.3. Los backups ¿se almacenan en un sitio con acceso restringido y suficientes medidas de seguridad? | X | | | |
| 2.8.4. ¿Se mantiene un backup periódico en un sitio externo? | X | | | |
| 2.8.5. ¿Se prueban los backups y su recuperación en forma periódica, para garantizar que cumplen con los requerimientos de los planes de continuidad de las actividades? | X | | | |
| **2.9. Preparación para recuperación ante contingencia:** | | | | |
| 2.9.1. ¿Se dispone de procedimientos documentados y aprobados para la recuperación del sistema ante fallas o contingencias? | | | | |
| 2.9.2. ¿Se realizan pruebas de recuperación periódicas? | X | | | |
| 2.9.3. ¿Se han definido claramente los roles y responsabilidades del equipo de trabajo encargado de la recuperación del sistema? | | X | | |
| **2.10. Análisis UAI:** | | | | |

| | | | | |
|---|---|---|---|---|
| 2.10.1. La UAI ¿ha realizado en los últimos 2 años un análisis sobre la calidad de los datos del sistema utilizando herramientas de TI a tal fin? (es decir, validar si los datos responden a los formatos y controles de los campos, verificar la presencia de inconsistencias, datos en blanco, etc.) (Nota: en caso afirmativo, indicar en Comentarios los informes que reflejan los resultados obtenidos) | X | | | |

De la información relevada en cada Sistema Informático, no surgen debilidades significativas que ameriten una observación.

## VII – Observaciones

No surgen observaciones que realizar.

## VIII – Recomendaciones

No surgen recomendaciones que realizar.

## IX – Opinión del sector auditado

No corresponde opinión del auditado.

## X – Conclusión

Los controles internos asociados a los sistemas informáticos y bases de datos críticas, que utiliza la Universidad Nacional de Moreno, resultan razonables en sus aspectos significativos, respecto de los controles mencionados en el Instructivo de Trabajo Nº 3/2017 – SLyT.

## XI – Lugar y fecha, firma y sello

**Buenos Aires,** 31 de agosto de 2017.