2017

SISTEMAS INFORMÁTICOS Y BASES DE DATOS CRÍTICAS

INFORME DE AUDITORÍA Nº 022/2017

Ministerio de
Trabajo, Empleo
y Seguridad Social

Unidad de Auditoría Interna

Ministerio de
Trabajo, Empleo
y Seguridad Social

UNIDAD DE AUDITORÍA INTERNA

Auditor Interno Titular
Lic. Ariel Ernesto DILEVA

Auditor Adjunto de Gestión de Recursos y Procesos de Apoyo
Dr. José Norberto DE NARDO

Supervisor de Auditoría de Tecnología de la Información
Lic. Maximiliano Antonio IORGI

Auditor Técnico
Sr. Alberto Carlos IGLESIAS

Contenido

INFORME ANALITICO

I) OBJETO	1
II) ALCANCE	1
III) ANTECEDENTES	1
IV) TAREA REALIZADA	2
V) DESCRIPCIÓN, OBSERVACIONES Y RECOMENDACIONES	2
VI) CONCLUSIÓN	5

APÉNDICE:

A. - INSTRUCTIVO DE TRABAJO N° 3/2017-SLyT – SIGEN – SISTEMAS INFORMÁTICOS Y BASES DE DATOS CRÍTICAS.

ANEXOS:

A. - RESUMEN GENERAL DE OBSERVACIONES.

INFORME DE AUDITORÍA ANALÍTICO

SISTEMAS INFORMÁTICOS Y BASES DE DATOS CRÍTICAS

I) OBJETO

Relevar los controles asociados a los Sistemas Informáticos y Bases de Datos Críticas, cuyo funcionamiento resulta indispensable para la ejecución de las funciones y operaciones del Ministerio de Trabajo, Empleo y Seguridad Social, brindando servicio a la ciudadanía, según lineamientos establecidos en el Instructivo de Trabajo Nº 3/2017-SLyT de la Sindicatura General de la Nación (SGN).

II) ALCANCE

La tarea fue realizada en el período comprendido entre los meses de junio y julio de 2017, de acuerdo con las Normas de Auditoria Interna Gubernamental aprobadas por Resolución SGN Nº 152/2002, aplicándose algunos de los procedimientos allí enumerados u otros que se consideraron necesarios en la circunstancia.

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

III) ANTECEDENTES

NORMATIVOS

- Ley N° 24.156 - Ley de Administración Financiera y de los Sistemas de Control del Sector Público Nacional.
- Decreto N° 1344/2007 – Aprueba el Reglamento de la Ley de Administración Financiera y de los Sistemas de Control del Sector Público Nacional N° 24.156;
- Resolución SGN N° 152/2002 – Aprueba las "Normas de Auditoría Interna Gubernamental".
- Resolución SGN N° 172/2014 – Aprueba las "Normas Generales de Control Interno".
- Circular N° 2/2017 – APN-SGN.
- Instructivo de Trabajo N° 3/2017-SLyT – SGN – Sistemas Informáticos y Bases de Datos Críticas.

Unidad Auditoría Interna MTEySS

DOCUMENTALES

- Copia de los Formularios del Instructivo de Trabajo N° 3/2017 – SLyT, realizados para cada Sistema Informático y Base de Datos Crítica.

IV) TAREA REALIZADA

Descripción

La tarea realizada consistió en la ejecución de los siguientes procedimientos de auditoría y/o verificaciones:

1. Análisis de la normativa aplicable;
2. Determinar los sistemas y bases de datos críticos de acuerdo con los criterios establecidos por la Dirección General de Informática e Innovación Tecnológica (DGIIT);
3. Relevar aspectos de control interno detallados en el Instructivo de Trabajo;
4. Completar los Formularios del Instructivo de Trabajo;
5. Evaluación de los resultados obtenidos;
6. Carga y envío de la información a la SGN a través del aplicativo dispuesto para tal fin en su intranet (https://net.sigen.gob.ar/IT2017/).

Sobre la base de los antecedentes relevados e información proporcionada por la DGIIT, en fecha 13 de julio de 2017 se procedió a la emisión del informe previsto en la Circular N°2/2017-APN - SGN y en el Instructivo de Trabajo N° 3/2017-SLyT – SGN para conocimiento de las autoridades del Organismo. Se adjunta al presente como **Apéndice A** copia de dicho informe.

Bajo el acápite "Respuesta del Sector Auditado", se incorporan al presente informe los comentarios efectuados por la DGIIT.

V) DESCRIPCIÓN, OBSERVACIONES Y RECOMENDACIONES

A continuación se describen los aspectos verificados, las observaciones surgidas de la labor y las recomendaciones que esta Unidad de Control sugiere sobre los sistemas informáticos que constituyeron materia de examen.

El relevamiento y auditoría de los controles internos que la SGN requiere a través del citado Instructivo de Trabajo, hacen foco en los sistemas informáticos y bases de datos críticas.

Unidad Auditoría Interna MTEySS

Luego de un análisis de criticidad se desarrolló la presente tarea sobre los siguientes Sistemas Informáticos y sus respectivas bases de datos:

1	ASISTIR
2	Crédito Fiscal
3	DNAS
4	Gestión Empleo
5	PNRT
6	REPRO
7	REPSAL
8	SECLO

Entre los principales aspectos de control verificados se encuentran los siguientes:

- Información Base de datos.
- Documentación Técnica del Sistema.
- Manual de Usuario del Sistema.
- Cambios a programas.
- Permisos de acceso al Sistema.
- Logs o Registros de Transacciones del Sistema.
- Acceso a datos
- Backup del Sistema.
- Preparación para recuperación ante contingencia.

A. - Información de Base De Datos

1. Observación

Si bien el Organismo ha definido los criterios para la clasificación de la información, se observa que aún está pendiente el cumplimiento de dicha tarea.

Recomendación

La DGIIT, por intermedio de la Dirección de Operaciones y Servicios y la Coordinación de Seguridad Informática, junto a las áreas responsables de los sistemas informáticos deben clasificar la información contenida en su base de datos y proceder a su documentación.

Respuesta del Sector Auditado

El Responsable Primario con la colaboración de la Dirección de Operaciones y Servicios y la Coordinación da Seguridad Informática debe identificar los recursos a su cargo y asignarles el nivel de clasificación de la información pertinente.

Fecha estimada: Marzo/2018

Unidad Auditoría Interna MTEySS

B. - Logs o Registros de Transacciones del Sistema

2. Observación

La Resolución MTEySS N° 267/2015 aprueba "El Manual de Reglas de Gestión para la Seguridad Informática". A la fecha del presente informe no se han aplicado tales reglas respecto de los logs o registros de transacciones de los sistemas.

Recomendación

La DGIIT, por intermedio de la Coordinación de Seguridad Informática, debe desarrollar las gestiones necesarias para la puesta en práctica de las reglas aprobadas oportunamente.

Respuesta del Sector Auditado

La CSI procederá a documentar el procedimiento y el estándar de Logs.

Fecha estimada: Marzo/2018

C. - Preparación para Recuperación ante Contingencia

3. Observación

La DGIIT no posee un Plan de Contingencia aprobado mediante acto administrativo que contenga, entre otros, los siguientes aspectos:

- Procedimientos determinados para la recuperación de sistemas
- Realización de pruebas en forma periódica
- Roles y responsabilidades del equipo que realizará esta tarea.

Recomendación

La DGIIT debe elaborar la documentación necesaria para la aprobación mediante acto administrativo de un Plan de Recuperación ante Contingencias para el Organismo, así como también debe evaluar la necesidad de un centro de cómputos alternativo dedicado a este fin.

Respuesta del Sector Auditado

La DGIIT está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.

Unidad Auditoría Interna MTEySS

Opinión UAI

De acuerdo con las respuestas brindadas, la DGIIT y las áreas que le dependen han receptado favorablemente las observaciones y las recomendaciones realizadas, estableciendo para cada caso un plan de trabajo y el desarrollo de acciones a efectos de su regularización. El efectivo cumplimiento de dichas acciones será verificado en próximas tareas de auditoría.

Resumen General de Observaciones

En el **Anexo A** se enumeran las observaciones descriptas precedentemente con el detalle para cada una de ellas de la siguiente información: a) Área y sub-área/s temática/s a las que se encuentran referidas; b) Calificación de impacto; c) Estado de situación; y d) Área Responsable que deben impulsar las acciones correctivas.

Resumen

Observaciones según su estado de situación				
Regularizada	**En Trámite**	**Sin Acción Correctiva**	**No Compartida**	**No Regularizable**
--*--	3	--*--	--*--	--*--
Total: 3 Observaciones				

VI) CONCLUSIÓN

Sobre la base de las tareas realizadas y sin perjuicio de las observaciones resultantes de los formularios de relevamiento, esta Unidad de Control estima que la Dirección General de Informática e Innovación Tecnológica cumple razonablemente los distintos aspectos contemplados en el Instructivo de Trabajo Nº 3/2017-SLyT – SGN – Sistemas Informáticos y Bases de Datos Críticas.

Por su parte, según surge de la opinión del sector auditado, ya se ha definido un plan de regularización y está impulsando una serie de acciones tendientes a subsanar las carencias detectadas.

Ciudad de Buenos Aires, 10 de agosto de 2017.

Lic. Maximiliano Antonio IORGI
Supervisor de Auditoría de Tecnología de la Información

Dr. CP José Norberto DE NARDO
Auditor Adjunto de Gestión de Recursos y Procesos de Apoyo

Lic. Ariel Ernesto DILEVA
Auditor Interno Titular

APÉNDICE A

Circular SIGEN N°2/2017 - SLyT - Instructivo de Trabajo N°3/2017-SLyT

UAI-MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL

Comprobante de auditoría finalizada

Sistemas auditados:

- Asistir
- Credito Fiscal
- DNAS
- Gestión Empleo
- PNRT
- REPRO
- REPSAL
- SECLO

Conclusiones:

Sobre la base de las tareas realizadas y sin perjuicio de las observaciones que han resultado del relevamiento, esta Unidad de Control estima que la Dirección General de Informática e Innovación Tecnológica cumple razonablemente los distintos aspectos contemplados en el Instructivo de Trabajo N° 3/2017 - SLyT - SGN: "Sistemas Informáticos y Bases de Datos Críticas".Por su parte, según surge de la opinión del sector auditado, ya se ha definido un plan de regularización y se está impulsando una serie de acciones tendientes a subsanar las carencias detectadas.

Comprobante:

Firma:	Aclaración:	Fecha: 13/07/2017
	Dr. JOSÉ NORBERTO DE NARDO AUDITOR ADJUNTO U.A.I.- M.T.E. y S.S.	

Informe detallado. (Numeración según puntos del Instructivo de Trabajo)

Nota: Solo se incluyen los puntos que presentaron incumplimiento Total o Parcial.

Nombre del sistema:

Credito Fiscal

2. CONTROL INTERNO

2.1. Información Base de datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
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)?	Parcialmente		El manual de reglas de gestión de Seguridad Informática aprobado por Res. SSC 267/15 contiene la RG "SSC-POI-DGIIT-14.04.05: Criterios de Clasificación de la Información" que contempla lo expuesto en la Disp. 1/2015 ONTI.	El Responsable Primario con la colaboración de la Dirección de Operaciones y Servicios y la Coordinación da Seguridad informática debe identificar los recursos a su cargo y asignarles el nivel clasificación de la información pertinente. Fecha estimada: 03/2018.

2.2. Documentación Técnica del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.3. Manual de Usuario del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.4. Cambios a programas:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.5. Permisos de acceso al Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.6. Logs o Registros de Transacciones del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
	Parcialmente			

2.6.2. ¿Existe un procedimiento documentado para el resguardo y análisis de los logs?			Se documentaron mediante Res. 267/15 los siguientes procedimientos:- SSC-POI-DGIIT-14.07.27 Registro y Auditoria de Controles de Seguridad.- SSC-POI-DGIIT-14.07.28 Protección de los registros de auditoria.- SSC-POI-DGIIT-14.08.06 Auditoria de recursos informáticos.	Documentar procedimiento y estándar de logs. Fecha estimada: 03/2018.

2.7. Acceso a datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.8. Backup del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.9. Preparación para recuperación ante contingencia:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.9.1. ¿Se dispone de procedimientos documentados y aprobados para la recuperación del sistema ante fallas o contingencias?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.
2.9.2. ¿Se realizan pruebas de recuperación periódicas?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.
2.9.3. ¿Se han definido claramente los roles y responsabilidades del equipo de trabajo encargado de la recuperación del sistema?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.

2.10. Análisis UAI:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
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)	NO		Ver Pautas Gerenciales para cada P.A.A.	Ver Plan Anual Ciclo de Auditoría.

Nombre del sistema:

Asistir

2. CONTROL INTERNO

2.1. Información Base de datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
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)?	Parcialmente		El manual de reglas de gestión de Seguridad Informática aprobado por Res. SSC 267/15 contiene la RG "SSC-POI-DGIIT-14.04.05: Criterios de Clasificación de la Información" que contempla lo expuesto en la Disp. 1/2015 ONTI.	El Responsable Primario con la colaboración de la Dirección de Operaciones y Servicios y la Coordinación da Seguridad informática debe identificar los recursos a su cargo y asignarles el nivel clasificación de la información pertinente. Fecha estimada: Marzo /2018.

2.2. Documentación Técnica del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.3. Manual de Usuario del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.4. Cambios a programas:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.5. Permisos de acceso al Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.6. Logs o Registros de Transacciones del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.6.2. ¿Existe un procedimiento documentado para el resguardo y análisis de los logs?	Parcialmente		Res. 267/15- SSC-POI-DGIIT-14.07.27 Registro y Auditoria de Controles de Seguridad.-	Documentar procedimiento y estándar de logs. Fecha estimada: Marzo/2018.

			SSC-POI-DGIIT-14.07.28 Protección de los registros de auditoria.- SSC-POI-DGIIT -14.08.06 Auditoria de recursos informáticos.	

2.7. Acceso a datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.8. Backup del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.9. Preparación para recuperación ante contingencia:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.9.1. ¿Se dispone de procedimientos documentados y aprobados para la recuperación del sistema ante fallas o contingencias?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.
2.9.2. ¿Se realizan pruebas de recuperación periódicas?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.
2.9.3. ¿Se han definido claramente los roles y responsabilidades del equipo de trabajo encargado de la recuperación del sistema?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.

2.10. Análisis UAI:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
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)	NO		Ver Pautas Gerenciales para cada P.A.A.	Ver Plan Anual Ciclo de Auditoría.

Nombre del sistema:

DNAS

2. CONTROL INTERNO

2.1. Información Base de datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
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)?	Parcialmente		El manual de reglas de gestión de Seguridad Informática aprobado por Res. SSC 267/15 contiene la RG "SSC-POI-DGIIT-14.04.05: Criterios de Clasificación de la Información" que contempla lo expuesto en la Disp. 1/2015 ONTI.	El Responsable Primario con la colaboración de la Dirección de Operaciones y Servicios y la Coordinación da Seguridad informática debe identificar los recursos a su cargo y asignarles el nivel clasificación de la información pertinente. Fecha estimada: Marzo/2018.

2.2. Documentación Técnica del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.3. Manual de Usuario del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.4. Cambios a programas:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.5. Permisos de acceso al Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.6. Logs o Registros de Transacciones del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.6.2. ¿Existe un procedimiento documentado para el resguardo y análisis de los logs?	Parcialmente		Se documentaron mediante Res. 267/15 los siguientes procedimientos:- SSC-POI-DGIIT-14.07.27 Registro y Auditoria de Controles de	Resta documentar el procedimiento y el estándar de logs. Fecha estimada: Marzo/2018.

			Seguridad.- SSC-POI-DGIIT-14.07.28 Protección de los registros de auditoria.- SSC-POI-DGIIT-14.08.06 Auditoria de recursos informáticos.	

2.7. Acceso a datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.8. Backup del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.9. Preparación para recuperación ante contingencia:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.9.1. ¿Se dispone de procedimientos documentados y aprobados para la recuperación del sistema ante fallas o contingencias?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos
2.9.2. ¿Se realizan pruebas de recuperación periódicas?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos
2.9.3. ¿Se han definido claramente los roles y responsabilidades del equipo de trabajo encargado de la recuperación del sistema?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos

2.10. Análisis UAI:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
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)	NO		Ver Pautas Gerenciales para cada P.A.A.	Ver Plan Anual Ciclo de Auditoría.

Nombre del sistema:

Gestión Empleo

2. CONTROL INTERNO

2.1. Información Base de datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
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)?	Parcialmente		El manual de reglas de gestión de Seguridad Informática aprobado por Res. SSC 267/15 contiene la RG "SSC-POI-DGIIT-14.04.05: Criterios de Clasificación de la Información" que contempla lo expuesto en la Disp. 1/2015 ONTI.	El Responsable Primario con la colaboración de la Dirección de Operaciones y Servicios y la Coordinación da Seguridad informática debe identificar los recursos a su cargo y asignarles el nivel clasificación de la información pertinente. Fecha estimada: Marzo/2018.

2.2. Documentación Técnica del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.3. Manual de Usuario del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.4. Cambios a programas:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.5. Permisos de acceso al Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.6. Logs o Registros de Transacciones del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.6.2. ¿Existe un procedimiento documentado para el resguardo y análisis de los logs?	Parcialmente		Se documentaron mediante Res. 267/15 los siguientes procedimientos:- SSC-POI-DGIIT-14.07.27 Registro y Auditoria de Controles de	Resta documentar el procedimiento y el estándar de logs. Fecha estimada: Marzo/2018.

			Seguridad.- SSC-POI-DGIIT-14.07.28 Protección de los registros de auditoria.- SSC-POI-DGIIT-14.08.06 Auditoria de recursos informáticos.	

2.7. Acceso a datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.8. Backup del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.9. Preparación para recuperación ante contingencia:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.9.1. ¿Se dispone de procedimientos documentados y aprobados para la recuperación del sistema ante fallas o contingencias?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.
2.9.2. ¿Se realizan pruebas de recuperación perlódicas?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.
2.9.3. ¿Se han definido claramente los roles y responsabilidades del equipo de trabajo encargado de la recuperación del sistema?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.

2.10. Análisis UAI:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

Nombre del sistema:

PNRT

2. CONTROL INTERNO

2.1. Información Base de datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.1.1. ¿Se ha clasificado la información administrada por el Sistema según su	Parcialmente		El manual de reglas de gestión de Seguridad	El Responsable Primario con la colaboración de la

nivel de criticidad, considerando lo expuesto en la Política de Seguridad Modelo aprobada mediante Disp. N° 1/2015 ONTI (Cláusula 8 – Gestión de Activos)?			Informática aprobado por Res. SSC 267/15 contiene la RG "SSC-POI-DGIIT-14.04.05: Criterios de Clasificación de la Información" que contempla lo expuesto en la Disp. 1/2015 ONTI.	Dirección de Operaciones y Servicios y la Coordinación da Seguridad informática debe identificar los recursos a su cargo y asignarles el nivel clasificación de la información pertinente. Fehca estimada: 03/2018.

2.2. Documentación Técnica del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.3. Manual de Usuario del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.4. Cambios a programas:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.5. Permisos de acceso al Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.6. Logs o Registros de Transacciones del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.6.2. ¿Existe un procedimiento documentado para el resguardo y análisis de los logs?	Parcialmente		Se documentaron mediante Res. 267/15 los siguientes procedimientos:- SSC-POI-DGIIT-14.07.27 Registro y Auditoria de Controles de Seguridad.- SSC-POI-DGIIT-14.07.28 Protección de los registros de auditoria.- SSC-POI-DGIIT-14.08.06 Auditoria de recursos informáticos.	Plan de acción: Documentar el procedimiento y el estándar de logs. Fecha estimada: 03/2018.

2.7. Acceso a datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	

				Curso de Acción Comprometido por el Auditado

2.8. Backup del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.9. Preparación para recuperación ante contingencia:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.9.1. ¿Se dispone de procedimientos documentados y aprobados para la recuperación del sistema ante fallas o contingencias?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.
2.9.2. ¿Se realizan pruebas de recuperación periódicas?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.
2.9.3. ¿Se han definido claramente los roles y responsabilidades del equipo de trabajo encargado de la recuperación del sistema?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.

2.10. Análisis UAI:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

Nombre del sistema:

REPRO

2. CONTROL INTERNO

2.1. Información Base de datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
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)?	Parcialmente		El manual de reglas de gestión de Seguridad Informática aprobado por Res. SSC 267/15 contiene la RG "SSC-POI-DGIIT-14.04.05: Criterios de Clasificación de la Información" que contempla lo expuesto en la Disp. 1/2015 ONTI.	El Responsable Primario con la colaboración de la Dirección de Operaciones y Servicios y la Coordinación da Seguridad Informática debe identificar los recursos a su cargo y asignarles el nivel clasificación de la información pertinente. Fecha estimada: Marzo/2018.

2.2. Documentación Técnica del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.3. Manual de Usuario del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.4. Cambios a programas:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.5. Permisos de acceso al Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.6. Logs o Registros de Transacciones del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.6.2. ¿Existe un procedimiento documentado para el resguardo y análisis de los logs?	Parcialmente		Se documentaron mediante Res. 267/15 los siguientes procedimientos:- SSC-POI-DGIIT-14.07.27 Registro y Auditoria de Controles de Seguridad.- SSC-POI-DGIIT-14.07.28 Protección de los registros de auditoria.- SSC-POI-DGIIT-14.08.06 Auditoria de recursos informáticos.	Resta documentar el procedimiento y el estándar de logs. Fecha estimada: Marzo/2018.

2.7. Acceso a datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.8. Backup del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.9. Preparación para recuperación ante contingencia:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.9.1. ¿Se dispone de procedimientos documentados y aprobados para la recuperación del sistema ante fallas o contingencias?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos
2.9.2. ¿Se realizan pruebas de recuperación periódicas?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos
2.9.3. ¿Se han definido claramente los roles y responsabilidades del equipo de trabajo encargado de la recuperación del sistema?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos

2.10. Análisis UAI:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
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)	NO		Ver Pautas Gerenciales para cada P.A.A.	Ver Plan Anual Ciclo de Auditoría.

Nombre del sistema:

REPSAL

2. CONTROL INTERNO

2.1. Información Base de datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
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)?	Parcialmente		El manual de reglas de gestión de Seguridad Informática aprobado por Res. SSC 267/15 contiene la RG "SSC-POI-DGIIT-14.04.05: Criterios de Clasificación de la Información" que contempla lo expuesto en la Disp. 1/2015 ONTI.	El Responsable Primario con la colaboración de la Dirección de Operaciones y Servicios y la Coordinación da Seguridad Informática debe identificar los recursos a su cargo y asignarles el nivel clasificación de la información pertinente. Fecha estimada: Marzo/2018.

2.2. Documentación Técnica del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	

				Curso de Acción Comprometido por el Auditado

2.3. Manual de Usuario del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.4. Cambios a programas:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.5. Permisos de acceso al Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.6. Logs o Registros de Transacciones del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.6.2. ¿Existe un procedimiento documentado para el resguardo y análisis de los logs?	Parcialmente		Se documentaron mediante Res. 267/15 los siguientes procedimientos:- SSC-POI-DGIIT-14.07.27 Registro y Auditoria de Controles de Seguridad.- SSC-POI-DGIIT-14.07.28 Protección de los registros de auditoria.- SSC-POI-DGIIT-14.08.06 Auditoria de recursos informáticos.	Resta documentar el procedimiento y el estándar de logs. Fecha estimada: Marzo/2018.

2.7. Acceso a datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.8. Backup del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.9. Preparación para recuperación ante contingencia:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.9.1. ¿Se dispone de procedimientos documentados y aprobados para la recuperación del sistema ante fallas o contingencias?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.
2.9.2. ¿Se realizan pruebas de recuperación periódicas?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.
2.9.3. ¿Se han definido claramente los roles y responsabilidades del equipo de trabajo encargado de la recuperación del sistema?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.

2.10. Análisis UAI:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
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)	NO		Ver Pautas Gerenciales para cada P.A.A.	Ver Plan Anual Ciclo de Auditoría.

Nombre del sistema:

SECLO

2. CONTROL INTERNO

2.1. Información Base de datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
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)?	Parcialmente		El manual de reglas de gestión de Seguridad Informática aprobado por Res. SSC 267/15 contiene la RG "SSC-POI-DGIIT-14.04.05: Criterios de Clasificación de la Información" que contempla lo expuesto en la Disp. 1/2015 ONTI.	El Responsable Primario con la colaboración de la Dirección de Operaciones y Servicios y la Coordinación da Seguridad informática debe identificar los recursos a su cargo y asignarles el nivel clasificación de la información pertinente. Fecha estimada: 03/2018.

2.2. Documentación Técnica del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	

				Curso de Acción Comprometido por el Auditado

2.3. Manual de Usuario del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.4. Cambios a programas:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.5. Permisos de acceso al Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.6. Logs o Registros de Transacciones del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.6.2. ¿Existe un procedimiento documentado para el resguardo y análisis de los logs?	Parcialmente		Se documentaron mediante Res. 267/15 los siguientes procedimientos:- SSC-POI-DGIIT-14.07.27 Registro y Auditoria de Controles de Seguridad.- SSC-POI-DGIIT-14.07.28 Protección de los registros de auditoria.- SSC-POI-DGIIT-14.08.06 Auditoria de recursos informáticos.	Plan de acción: Documentar el procedimiento y el estándar de logs. Fecha estimada: 03/2018.

2.7. Acceso a datos:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.8. Backup del Sistema:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado

2.9. Preparación para recuperación ante contingencia:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
2.9.1. ¿Se dispone de procedimientos documentados y aprobados para la recuperación del sistema ante fallas o contingencias?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.
2.9.2. ¿Se realizan pruebas de recuperación periódicas?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.
2.9.3. ¿Se han definido claramente los roles y responsabilidades del equipo de trabajo encargado de la recuperación del sistema?	Parcialmente		A la espera del resultado del curso de acción establecido.	Se está evaluando una alternativa para contar con un centro de cómputos en ARSAT para estos casos.

2.10. Análisis UAI:

Aspecto a Verificar	Cumple	Comentarios	Opinión del Auditado	Curso de Acción Comprometido por el Auditado
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)	NO		Informe N° 013/2014 - SECLO-WEB.	Ver Plan Ciclo de Auditoría.

ANEXO A

RESUMEN GENERAL DE OBSERVACIONES [1]

Nº de Orden	Área Temática	Sub-Área Temática	Calificación de Impacto			Estado de Situación [2]					Área/s Responsable/s[3]
			Alto	Medio	Bajo	R	ET	SAC	NC	NR	
1	Proceso de Apoyo	Sistemas			X		X				DGIIT
2	Proceso de Apoyo	Sistemas			X		X				DGIIT
3	Proceso de Apoyo	Sistemas		X			X				DGIIT

[1] Incorporadas en el Sistema de Seguimiento de Informes y Observaciones (SISIO).
[2] Referencias: (R) Regularizada / (ET) En Trámite / (SAC) Sin Acción Correctiva / (NC) No Compartida / (NR) No Regularizable.
[3] Unidades Organizativas que deben impulsar acciones correctivas respecto de la observación formulada. Referencia: (DGIIT) Dirección General de Informática e Innovación Tecnológica.

Unidad Auditoría Interna MTEySS

Unidad de Auditoría Interna

Avenida Leandro N. Alem 650, piso 3º
(1001AAO), Ciudad Autónoma de Buenos Aires
Tel. 4310-6175 Fax: 4310-6169
E-mail: uauditor@trabajo.gob.ar

Ministerio de
Trabajo, Empleo
y Seguridad Social