INFORME DE SEGUIMIENTO FINAL

TECNOLOGÍA DE LA INFORMACIÓN ENTREGA Y SOPORTE

ANÁLISIS MANEJO DE INFORMACIÓN EN PLATAFORMA RDIC

CSI 15/2019

Palabras Clave	Ciclo de Vida del Desarrollo - Módulos, Roles y Perfiles - Pistas de Auditoría (Logs) - Seguridad

Hipólito Yrigoyen 370 Piso 5 Of. 5123 (1086) CABA- 11 4347-4135 (RPG 4135)- auditoriainterna@afip.gob.ar

Índice del Informe

SÍNTESIS EJECUTIVA

FUNDAMENTOS DE LA AUDITORÍA

Se trata de una auditoría planificada, destinada a obtener conclusiones respecto del ciclo de vida del desarrollo seguro de la plataforma RDIC, llevado a cabo por SDG SIT, para garantizar la seguridad de la información que la misma contiene.

IMPACTO EN EL ORGANISMO

La presente actividad de la UAI contribuye al logro de los siguientes objetivos estratégicos e institucionales de esta Administración Federal:

-Facilitar el cumplimiento.

-Administrar con eficiencia los recursos.

Es menester de las tareas de la auditoría colaborar con el Organismo para fortalecer los mecanismos de protección de los datos y su adecuado, controlado y eficiente procesamiento y disponibilidad para garantizar a los ciudadanos la transparencia y equidad esperada, redundando en la calidad del servicio.

EFECTIVIDAD DEL SISTEMA DE CONTROL

En base a la evaluación efectuada sobre la efectividad del Sistema de Control Interno, se concluye que el mismo es:

- ⇒ **Deficiente/Inexistente**
- ⇒ Regular
- ⇒ Más que Regular
- ⇒ Bueno
- ⇒ Óptimo

ESTADO DE SITUACIÓN DE LAS OBSERVACIONES Y RECOMENDACIONES DE AUDITORÍA INTERNA

En función de las tareas de seguimiento efectuadas sobre los hallazgos de la auditoría relacionados con aspectos de seguridad y cumplimiento de las normas vigentes respecto del ciclo de vida de desarrollo de la Plataforma RDIC, se verificó que, si bien se ha formalizado una nueva normativa referida al ciclo de software que contempla la documentación obligatoria y opcional que debe ser producida en cada una de las etapas, no se han especificado pruebas de cumplimiento funcional, ni requisitos y controles mínimos que debe tener un nuevo desarrollo de sistemas o una nueva funcionalidad para encontrarse en condiciones de ser implementada en el ambiente de producción.

Adicionalmente, no se ha evidenciado la definición de un procedimiento de reválida y depuración periódica de usuarios con privilegios, ni la implementación de un control periódico de asignación de los roles y perfiles críticos que poseen la capacidad de consultar la información completa de la DDJJ de los agentes, administrar las matrices de riesgo y/o generar reportes desde el aplicativo.

Las situaciones expuestas representan un riesgo elevado de que se produzcan accesos indebidos a información sensible del personal del Organismo.

Por otra parte, considerando que, mediante la Disposición N.° 140/2020 (AFIP), se eliminó de la estructura orgánica de la AFIP a la ex Dirección de Integridad Institucional y sus unidades dependientes, se incorpora como área destinataria al Comité de Integridad y Ética Pública a los efectos de que tome conocimiento, en el marco de sus competencias, de los hallazgos vertidos en el presente informe.

Asimismo, teniendo en cuenta que mediante la mencionada Disposición fue derogada la Disposición N.° 353/2017 (AFIP) – "Régimen Declarativo de Información Confidencial (RDIC)", en caso de discontinuar el uso de la herramienta informática, se destaca la necesidad de que se impulsen las acciones que estipula la Instrucción General N° 1/2019 SDG SIT - "Pautas para el Desarrollo, Mantenimiento y Discontinuidad de los Sistemas Informáticos de la AFIP".

ÁREAS RESPONSABLES DE IMPLEMENTACIÓN DE ACCIONES

- ⇒ Subdirección General de Sistemas y Telecomunicaciones
- ⇒ Comité de Integridad y Ética Pública

Ciudad Autónoma de Buenos Aires.

Destinatarios

- Subdirección General de Sistemas y Telecomunicaciones
- Comité de Integridad y Ética Pública

Objeto

- Analizar y obtener conclusiones acerca del ciclo de vida del desarrollo de la plataforma RDIC, focalizando en los aspectos de seguridad más relevantes.

Tipo de auditoría

- Según su origen: Planificada
- Según su extensión: Operacional
- Según su temática: de Sistemas Informáticos

Reserva documental

En cumplimiento de lo establecido por los artículos 1°; 7° inciso a) y 32 inciso i), concordantes y complementarios de la Ley N.°27.275 de Derecho de Acceso a la Información Pública, las actuaciones vinculadas a la presente auditoría, mantendrán el carácter de "Reservado", asignado por la Disposición DI-2018-8-E-AFIP-AFIP, hasta la fecha en que sea incorporado en la base de datos del micrositio "Transparencia Activa" el Informe de Seguimiento Final o el último Informe de Auditoría correspondiente a la misma.

En tal sentido, hasta que se verifique dicha incorporación, el contenido de los Informes de Auditoría y de las actuaciones relacionadas a los mismos sólo serán de acceso pleno para las áreas auditadas, las áreas de las que ellas dependan y demás dependencias responsables de la regularización de los desvíos observados, incluidas las autoridades superiores del Organismo en función de sus competencias.

El acceso al contenido de los mismos por parte de una dependencia distinta, cuando existan motivos que justifiquen tal proceder, deberá ser expresamente habilitado por la Subdirección General de Auditoría Interna, a fin de evitar la indebida divulgación de la información vinculada con asuntos de criticidad institucional durante la sustanciación de la auditoría, con fundamento en lo normado en la disposición referida anteriormente.

En virtud de lo establecido en el artículo 32 inciso i) de la Ley N.°27.275, la publicación en el micrositio "Transparencia Activa" del último Informe de Auditoría de la auditoría en cuestión se efectuará con ajuste a las previsiones del artículo 8° de la citada ley, con estricto cumplimiento de los institutos de secreto fiscal (art. 101 Ley N.°11.683) y de estadística (art. 10 Ley N.°17.622), y la protección de los datos personales sensibles (Ley N.°25.326); en función de lo instruido sobre el tema por la Sindicatura General de la Nación.

El contenido de este documento es exclusivo para el/los destinatario/s, y puede contener información amparada por los institutos de "Secreto Fiscal" (Ley N.°11.683, artículo 101; Disposición AFIP N.°98/09 e Instrucción General AFIP N.°08/06, y sus modif.), "Estadística" (Ley N.°17.622, artículo 10) y "Protección de Datos Personales" (Ley N.°25.326, artículo 10).

En consecuencia, para su remisión a terceros deberá contar ineludiblemente con la conformidad expresa del remitente; en el caso de instancias internas del Organismo, la misma será exteriorizada de acuerdo lo establecido por la Disposición DI-2018-8-E-AFIP-AFIP, y para las externas a la AFIP, conforme las previsiones contenidas al efecto por las normas referidas en el párrafo anterior.

Finalmente, para los supuestos en que su divulgación sea requerida con fundamento en la competencia específica de la instancia solicitante, debidamente acreditada, se evaluará la solicitud en función de lo expresado anteriormente, resolviéndose lo que corresponda en cada caso, con el objeto de satisfacer -en la medida de lo posible- la misma.

Marco de referencia

La plataforma RDIC (Régimen Declarativo de Información Confidencial) es un formulario de carga, en el cual se solicita al declarante información propia y sobre su entorno familiar. Dicho formulario posee carácter de declaración jurada de información confidencial y se encuentra organizado en cinco módulos (compromisos éticos, grupo familiar, cargos y actividades, intereses económicos y aspectos penales). Para completar la información correspondiente a cada uno de los módulos, el declarante dispondrá de campos de validación simple, de opciones múltiples, y abiertos.
La plataforma plantea un recorrido de seis etapas, considerándose a la última de ellas como una instancia de revisión, la cual le permitirá verificar los contenidos de cada módulo previo a realizar la presentación de la declaración jurada. La información proporcionada tendrá carácter confidencial, se encuentra alcanzada por los institutos del secreto fiscal y el secreto profesional y se encuentra protegida legalmente contra su divulgación. Según los fines para los cuales ha sido desarrollada la plataforma, la información proporcionada será utilizada con la exclusiva finalidad de prevenir y evaluar eventuales situaciones que comprometan los deberes y pautas de comportamiento ético aplicables a los agentes del Organismo.

Alcance

Las tareas se desarrollaron según la metodología establecida por el Manual de Auditoría Interna de la Unidad de Auditoría Interna de la Administración Federal de Ingresos Públicos en un todo de acuerdo con las Normas de Auditoría Interna Gubernamental (Resolución SIGEN N.°152/02) en el marco de la Ley N.°24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional.

El trabajo abarcó el relevamiento y análisis del cumplimiento de la normativa aplicable y las actividades y procedimientos de control relativos a la gestión del análisis y manejo de información de la Plataforma RDIC por el período comprendido entre el 06 de noviembre de 2017 y el 31 de julio de 2018 (*Unidad auditable y Normativa aplicable en el Anexo A*).

Las tareas de seguimiento se llevaron a cabo entre el 28 de junio de 2019 y el 07 de julio de 2021 (*mayor detalle en el Anexo B*).

Se solicitó la opinión del/las área/s auditada/s y/o con injerencia en el tema aquí tratado (*mayor detalle en el Anexo C*).

El presente informe se encuentra referido a las observaciones, efectos y opiniones sobre el objeto de la tarea realizada hasta el 07 de julio de 2021 y no contempla la eventual ocurrencia de hechos posteriores que puedan modificar su contenido.

Las observaciones y/o hallazgos presentados en este informe corresponden a la situación observada al momento de realizar el trabajo. Al ser el control interno y su ejecución, aspectos dinámicos y dependientes en mayor o menor medida de factores humanos, existe un margen de riesgo que no puede ser cubierto en su totalidad.

El trabajo realizado incluyó un análisis de pistas electrónicas –ya sean pistas de auditoría, registros de eventos en los sistemas, archivos generados en los sistemas, etc., basándose en el principio de confianza en que toda información suministrada por los responsables es íntegra, completa y veraz.

La evaluación de la efectividad del control de aquellos riesgos que se han pretendido mitigar ayuda a disuadir la concreción de fraude. Cabe aclarar, que en el desempeño de la labor de auditoría pueden realizarse pruebas adicionales dirigidas a la identificación de indicadores de fraude ante deficiencias significativas de control, así como proceder a informar situaciones presuntamente anómalas o irregulares detectadas en las tareas de auditoría que resulten contrarias a los valores, principios básicos y pautas de comportamiento según lo establecido en el Código de Ética y demás normativa vigente en la materia, para su eventual evaluación por parte del área pertinente.

Al momento de la emisión del Informe Preliminar de Auditoría Interna, era responsabilidad de la ex Dirección de Integridad Institucional la prevención e investigación de aquellas conductas de los agentes que resultaren contrarias a los deberes y pautas de comportamiento ético. Debido a los cambios surgidos conforme las Disposiciones N.°140/2020 (AFIP) y N° 191/2020 (AFIP), las mismas serán informadas a la SDG AUI para su evaluación.

Se deja constancia que el presente no constituye un dictamen técnico y/o jurídico ni instrucción de servicio, los cuales deberán ser expedidos por las instancias de gestión competentes. Se procura poner en conocimiento de las áreas de gestión, desvíos o posibles desvíos para que éstas analicen si comparten esa calificación y, en su caso, decidan la adopción de cursos de acción correctivos, tomando en cuenta los sugeridos por la Subdirección General de Auditoría Interna, o si están dispuestas a asumir el riesgo que los mismos implican.

Aclaraciones previas

La ex Dirección de Integridad Institucional y sus unidades dependientes fueron eliminadas de la estructura organizativa de AFIP a través de la Disposición N.° 140/20 (AFIP) con vigencia a partir de los diez (10) días corridos contados desde el 14 de agosto de 2020, día de su publicación en el Boletín Oficial.

En su reemplazo, se creó un Comité denominado “Comité de Integridad y Ética Pública”, integrado por los Subdirectores Generales de las Subdirecciones Generales de Coordinación Técnico Institucional, Asuntos Jurídicos, Auditoría Interna, Recursos Humanos y Planificación, con competencia para asegurar la aplicación de la normativa vigente en materia de integridad y ética, proponer la elaboración de normas afines, definir las directrices de los programas de capacitación y promoción sobre dicha temática y promover la observancia de los valores, principios básicos y pautas que deben orientar la conducta de los agentes del Organismo, entre otras funciones. Asimismo, y con el objetivo de asistir al mencionado Comité en el cumplimiento de sus funciones, se creó la Dirección Ejecutiva del Comité de Integridad y Ética Pública.

Con relación a las tareas que le fueron asignadas a la ex Dirección de Integridad Institucional, se dispuso que vuelvan a ser desempeñadas por las Subdirecciones Generales de Auditoría Interna y de Recursos Humanos en el marco de las responsabilidades primarias que les fueron conferidas oportunamente por el Decreto N.° 898/05 (PEN).

En la misma normativa, se derogaron las Disposiciones N.° 353/2017 (AFIP) – Régimen Declarativo de Información Confidencial (RDIC), N.° 362/2017 (AFIP), N.° 119/2018 (AFIP), la Instrucción General N.° 8/2017 (AFIP) y la Instrucción General Conjunta N.° 1/2017 (DI INIT - SDG SIT) citadas en el Marco de Referencia del presente informe. Del mismo modo, quedaron derogadas las Disposiciones N.° 293/2018 (AFIP) - Política de no represalias y confidencialidad de la información de la AFIP y N.° 152/2019 (AFIP) - Sistema de Reporte de Agentes vinculados a Causas Penales (RACAP).

El Informe Preliminar de Auditoría Interna fue emitido el 03 de abril de 2019; el Informe de Auditoría Interna fue emitido el 28 de junio de 2019.

Con la emisión del presente informe se procede al archivo de las actuaciones.

Análisis del SCI

El Sistema de Control Interno es un proceso llevado a cabo no sólo por las autoridades superiores del Organismo, sino por la totalidad de los agentes pertenecientes al mismo, diseñado con el objetivo de proporcionar un grado de seguridad razonable en cuanto a la consecución de los objetivos organizacionales.

La Sindicatura General de la Nación (SIGEN) ha definido -mediante la Resolución N.°172/14 (SGN)- las Normas Generales de Control Interno; en las mismas se pueden encontrar los Componentes del Control Interno y, en un mayor grado de detalle, los principios y normas específicas que los constituyen. Cada norma específica posee su propio grado de Prioridad/Nivel de Madurez, que va de una escala de UNO (mayor prioridad o menor nivel de madurez) a CUATRO (menor prioridad o mayor nivel de madurez) según la importancia que revista.

En tal sentido, corresponde a esta Subdirección General de Auditoría Interna determinar el grado de apartamiento del control interno respecto del grado razonable de seguridad esperado. Para ello, se definió una escala de seis grados (nulo, mínimo, bajo, moderado, alto y extremo).

Vista la norma emanada por SIGEN, y considerando la labor desarrollada por esta Auditoría Interna, se concluye que los Componentes del Control Interno más representativos de los procesos, y su grado de apartamiento respecto del grado razonable de seguridad esperado, son:

Componentes del Control Interno	Control Auditado (*)	Prioridad y Apartamiento
Componente 3 - ACTIVIDADES DE CONTROL		
Principio 11 - DEFINICIÓN E IMPLEMENTACIÓN DE CONTROLES		
11.3 Seguridad de la información.	2.1	1
11.4 Controles de acceso sobre los recursos.	2.1	2
Principio 12 - POLÍTICAS Y PROCEDIMIENTOS		
12.1 Definición de políticas y procedimientos.	1.2	1
12.2 Aplicación de controles especificados en políticas y procedimientos.	1.2 - 2.1	1
12.3 Asignación de responsabilidades y mecanismos de rendición de cuentas.	2.1	**3**

(*) Mayor detalle en Anexo A - Unidad auditable.

Referencias:

Prioridad/Nivel de Madurez. Escala:

1	2	3	4

Nivel definido para el componente/principio/norma mediante la Resolución N.°172/14 (SGN)

Grado de apartamiento del Nivel de Madurez según el Principio involucrado:

NULO	MÍNIMO	BAJO	MODERADO	ALTO	EXTREMO

Verde: Nulo. *Aspecto eficiente. Los controles asociados mitigan razonablemente los riesgos relevantes.*
Verde claro: Mínimo*. Aspecto susceptible de mejora. Acción correctiva con intervención no prioritaria.*
Amarillo: Bajo. *Situación poco deficiente. Acción correctiva con intervención de prioridad baja.*
Naranja: Moderado. *Situación deficiente. Acción correctiva con intervención de prioridad intermedia.*
Rojo: Alto. *Elevado nivel de riesgo. Acción correctiva de intervención prioritaria.*
Bordó: Extremo. *Alto nivel de riesgo. Acción correctiva de intervención inmediata.*

La ponderación de ambas variables (prioridad y grado de apartamiento) permite planificar la implementación de mejoras mediante un esquema escalonado, atendiendo en lo inmediato los aspectos que impliquen una mayor criticidad, que se ve reflejada en la prioridad determinada. Mediante la siguiente grilla se brinda al área responsable con competencia una clasificación más específica sobre la preeminencia que debe tener el tratamiento de cada observación respecto de las demás:

Clasificación de observaciones vertidas en el cuerpo analítico del Informe						
SIGEN \ SDG AUI		Criticidad del Riesgo Residual				
		MÍNIMA	BAJA	MODERADA	ALTA	EXTREMA
Prioridad / Nivel de Madurez	1					1
	2					2 - 3
	3					
	4					

Detalle de Observaciones, Causas, Efectos y Recomendaciones

1. Controles insuficientes para pase a producción

Observación

En la Instrucción General N.° 05/2012 (SDG SIT) – *"Procedimiento para la documentación del desarrollo, mantenimiento y discontinuidad de los Sistemas Informáticos de la AFIP"*, vigente al momento del desarrollo e implementación de la Plataforma RDIC, en la sección III *"Responsables"*, indica al Área de Control de Calidad como *"área informática responsable de planificar, coordinar y desarrollar las actividades que aseguren la calidad del proceso de desarrollo de software incluyendo, de corresponder, la puesta en producción"*.

Durante el relevamiento, se pudo observar que los controles realizados en forma previa a la puesta en producción de la Plataforma RDIC no resultaron suficientes para concluir que la misma se encuentra en condiciones de ser migrada a un entorno productivo, ni para garantizar que su esquema de seguridad sea apropiado. Según la documentación relevada y las consultas realizadas, no se han llevado a cabo, por ejemplo, controles sobre la correspondencia de los roles y perfiles definidos en el proyecto inicial con los mismos definidos y asignados en la plataforma, así como tampoco revisiones de código fuente, test de estrés y test de volumen. A pesar de dicha situación, se pudo observar que la Plataforma RDIC se encuentra actualmente en estado Productivo y funcionando.

Durante la entrevista de cierre llevada a cabo el 29 de abril de 2019, el Departamento Certificación de la Calidad de los Sistemas (DI ECCS) señaló que *"manifiestan estar de acuerdo con lo observado y que actualmente se encuentra en etapa de implementación de los controles mencionados. Plazo estimado 30 días hábiles"*.

Causa

Incumplimiento de las misiones y funciones de las áreas involucradas.

Falta de apego a la normativa vigente.

Efecto

Posibilidad que la Plataforma RDIC no cumpla con los requisitos mínimos para su puesta en producción.

Potencial filtración de información sensible y confidencial del personal perteneciente del Organismo.

Recomendación

Formalizar e institucionalizar a través de una normativa los requisitos mínimos y los controles que debe cumplir un nuevo desarrollo para certificar su paso a producción.

Atento al tiempo que puede requerir la implementación de lo recomendado, se sugiere al Departamento Certificación de la Calidad de los Sistemas (DI ECCS) someter, a la brevedad, a la Plataforma RDIC a una revisión de cumplimiento de los requisitos mínimos y los controles que debe cumplir un nuevo desarrollo para certificar su paso a producción establecidos en el primer párrafo de la presente recomendación.

Plan de acción

Área Responsable con Competencia	Fecha prevista
Dirección de Tecnología y Arquitectura de los Sistemas (SDG SIT)	

Opinión/Plan de Acción del Auditado/Responsable con Competencia

La Dirección de Tecnología y Arquitectura de los Sistemas (SDG SIT), mediante correo electrónico del 14/05/2020, manifestó: *"En consonancia a la respuesta ya remitida para esta observación, presente en la Nota N.° 39/2019 (DI ECCS) de fecha 28/06/2019, Dirección de Tecnología y Arquitectura de los Sistemas (ex DI ECCS) hace saber a esa UAI que, a través del Departamento Arquitectura de los Sistemas (DE ARSI) se ha cumplimentado con la elaboración de la nueva normativa referida al proceso del Ciclo de Vida del Proceso de Desarrollo de Software. Formalizada a través de IG N.° 01/2019 SDG SIT "Pautas para el Desarrollo, Mantenimiento y Discontinuidad de los Sistemas Informáticos de la AFIP"; y en donde se incorporan los requisitos mínimos y controles pertinentes que deben ser cumplidos en todo desarrollo de software.*

Asimismo, se comunica que el Departamento Calidad de los Sistemas (DE CASI) ha realizado, de acuerdo a la normativa vigente, las certificaciones de calidad de documentación y análisis estático de código fuente de las implementaciones de la aplicación en cuestión; encontrándose las mismas informadas en las peticiones de Redmine Central y Redmine Unificado correspondiente […]".

Opinión de Auditoría Interna

Atento a la respuesta brindada, este servicio de auditoría considera que, si bien la normativa contempla la documentación obligatoria y opcional que debe ser producida en el ciclo de vida de desarrollo de software, no detalla cuales deben ser las pruebas de cumplimiento funcional, los requisitos y los controles mínimos con los que debe cumplir un nuevo desarrollo de sistemas o una

nueva funcionalidad, en cada una de las etapas del ciclo, para su pasaje a producción.

Por otro lado, se destaca que, si bien las actividades de calidad remitidas por la Dirección de Tecnología y Arquitectura de los Sistemas (SDG SIT) se encuentran relacionadas con el análisis estático del código fuente y la validación de documentación de la aplicación dentro del ciclo de vida de desarrollo, no resultan pertinentes para regularizar la presente observación debido a que corresponden a la implementación de dos nuevas funcionalidades y no a una revisión integral de calidad de la Plataforma RDIC, tal como fue recomendado.

En virtud de ello, teniendo en cuenta que mediante la Disposición N.° 140/2020 (AFIP) fue derogada la Disposición N.° 353/2017 (AFIP) – "Régimen Declarativo de Información Confidencial (RDIC)", y contemplando que la presente observación se encuentra incluida en el cargo *CSI 18/2020 – Gestión de cambios en aplicaciones*, en caso de no ser discontinuada la herramienta, el seguimiento del presente hallazgo se realizara mediante el mencionado cargo.

Criticidad del Riesgo Residual					Efectividad del Control Interno					Estado de la observación
Ext	Alt	Mod	Baj	Mín	Def/In	Reg	MRe	Bue	Ópt	No regularizable

2. Incorrecta asignación de roles y perfiles

Observación

En el Anexo I del Manual de Políticas de Seguridad de la Información (Disposición AFIP N.° 76/2005), vigente al momento del desarrollo e implementación de la Plataforma RDIC, en la sección "Administración de Acceso Lógico", subsección "Habilitación de Accesos", se establece: *"La habilitación de accesos sólo deberá ser generada para aquellos […] cuya necesidad de uso esté debidamente justificada por la índole de sus tareas, comprendiendo tanto el uso de las aplicaciones específicas como de cualquier otro programa que permita el acceso a los recursos"*.

Al mismo tiempo, en el Anexo de la Política de Seguridad de la Información (Disposición AFIP N.° 29/2019), vigente al momento de emisión del presente informe, en la sección "Gestión de Accesos", subsección "Habilitación de Accesos", se establece: *"La habilitación de accesos solo deberá ser generada para aquellos que lo hubieran solicitado […] y cuya necesidad de uso esté debidamente justificada acorde con sus tareas y funciones […]"*.

Durante el relevamiento, no se pudo observar la existencia de un control periódico de asignación de roles y perfiles respecto de la Plataforma RDIC. En consecuencia, el 80% de los usuarios del sistema (4 de un total de 5) no poseen correctamente asignados los roles y perfiles, según lo establecido en la Especificación de Requerimientos de Software (ERS) emitida por el área definidora.

En los comentarios expresados en la minuta de cierre remitida el 26 de abril de 2019, la Dirección de Integridad Institucional señaló que "*Los roles y perfiles actualmente asignados respecto de la Plataforma RDIC, son el resultado de un intercambio dinámico propiciado entre esta Dirección y las áreas intervinientes de la SDG SIT, a fin de asegurar los compromisos asumidos por esta Administración Federal. Al respecto, se destaca que el documento al que refiere dicho cuerpo auditor y aportado por esta DI INIT - Especificación de Requerimientos de Software (ERS) – corresponde a una versión borrador trabajada al inicio del intercambio anteriormente mencionado, no contando con la versión definitiva. En relación a ello, se informa que los roles y perfiles del 100% de los usuarios se encuentran correctamente asignados, garantizando con ello los estándares de seguridad de acceso a la información oportunamente definidos".*

Causa

Falta de apego a la normativa vigente.

Incorrecta definición de reglas de solicitud de usuarios.

Efecto

La falta de control y actualización de los roles y perfiles asignados a los usuarios de la Plataforma RDIC podría redundar en el acceso indebido a información sensible del personal del Organismo, poniendo en riesgo la confidencialidad de la información.

Potencial filtración de información sensible y confidencial del personal perteneciente al Organismo.

Recomendación

Realizar y formalizar una adecuada definición de roles y perfiles, y ajustar con celeridad la asignación de cada uno de ellos a los usuarios de la Plataforma RDIC.

Al mismo tiempo, se recomienda definir un esquema de reglas de solicitud de usuarios que permita que únicamente los usuarios correspondientes puedan solicitar los roles y perfiles asociados a sus tareas y funciones.

Plan de acción

Área Responsable con Competencia	Fecha prevista
Dirección de Integridad Institucional	-

Opinión/Plan de Acción del Auditado/Responsable con Competencia

La Dirección de Integridad Institucional, mediante el documento *"Plan de remediación: Acciones mitigantes de riesgos residuales"* adjunto al correo electrónico N° 131/2019 del 19/11/2019, manifestó: *"En cuanto a los roles y perfiles asignados respecto de la plataforma RDIC, que los mismos resultan correctos desde el punto de vista del uso de la herramienta. No obstante ello, y en vías de otorgar una solución a las observaciones planteadas, esta Dirección se comprometió a adecuar y formalizar la definición de los roles y perfiles, ajustando la asignación de cada uno de ellos a los usuarios de la plataforma RDIC. Consecuentemente, con el objetivo de atender los aspectos planteados por el Servicio de Auditoría, se adecuó el documento de "Especificaciones de Requerimientos de Software"*.

Opinión de Auditoría Interna

Considerando que mediante la Disposición N° 140/2020 (AFIP), se eliminó de la estructura orgánica de la AFIP a la ex Dirección de Integridad Institucional y sus unidades dependientes, y teniendo en cuenta que mediante la mencionada Disposición fue derogada la Disposición N° 353/2017 (AFIP) – "Régimen Declarativo de Información Confidencial (RDIC)", se debería evaluar la discontinuación de la herramienta y el resguardo de la información procesada durante su período de vigencia, conforme lo indica la Instrucción General N°1/2019 – "Pautas para el Desarrollo, Mantenimiento y Discontinuidad de los Sistemas Informáticos de la AFIP" (SDG SIT).

A instancias del presente informe de Seguimiento, esta Unidad de Auditoría verificó que no existen accesos otorgados sobre la herramienta RDIC, y que no se han registrado eventos en la tabla de auditoría en forma posterior a la derogación mencionada.

Finalmente, hasta tanto se defina lo mencionado en los párrafos precedentes, el estado de la presente observación quedará a verificar en futuras auditorías.

Criticidad del Riesgo Residual					Efectividad del Control Interno					Estado de la observación
Ext	Alt	Mod	Baj	Mín	Def/In	Reg	MRe	Bue	Ópt	Con acción correctiva informada

3. Existencia de perfiles no definidos

Observación

La Instrucción General N° 05/2012 (SDG SIT) – "Procedimiento para la documentación del desarrollo, mantenimiento y discontinuidad de los Sistemas Informáticos de la AFIP", vigente al momento del desarrollo e implementación de la Plataforma RDIC, en la sección III "Responsables", indica al Área Homologadora como responsable de efectuar las pruebas de homologación de los desarrollos de software realizados. Al mismo tiempo, en la sección VII "Resumen", subsección 6 "Documento de Pase a Producción", se detalla el objetivo de *"Especificar la puesta efectiva en producción del sistema y registrar la conformidad del pase a producción del Área Homologadora"*. En la misma dirección, en la sección VII "Resumen", subsección 7 "Informes de Prueba", se detalla el objetivo del Área de Control de Calidad de *"Registrar las pruebas realizadas sobre el software desarrollado"*, especificando que dichos informes deben realizarse para cada tipo de prueba, incluyendo las pruebas de accesos.

Durante el relevamiento no se pudo evidenciar la existencia de un control que garantice la correcta implementación del esquema de actores y responsabilidades establecido por el área definidora en la Especificación de Requerimientos de Software (ERS). En consecuencia, existen tres roles que no se encuentran determinados en el documento. A detallar:

- Rol "ADMINISTRACION DE MATRICES DE RIESGOS"
- Rol "REPORTE DE ACTIVIDADES DECLARADAS"
- Rol "REPORTE DE FAMILIARES QUE TRABAJAN EN AFIP"

En los comentarios expresados en la minuta de cierre remitida el 26 de abril de 2019, la Dirección de Integridad Institucional señaló que *"los roles definidos, son el resultado de un intercambio dinámico propiciado entre esta Dirección y las áreas intervinientes de la SDG SIT, a fin de asegurar los compromisos asumidos por esta Administración Federal. Al respecto, se destaca que el documento al que refiere dicho cuerpo auditor aportado por esta DI INIT - Especificación de Requerimientos de Software (ERS) – corresponde a una versión borrador trabajada al inicio del intercambio anteriormente mencionado, no contando con la versión definitiva. Finalmente, se aclara que los mismos corresponden a los roles definidos en el marco de las tareas correspondientes al apartado 5. Alcance del punto Próximas Etapas del "Acta Acuerdo de Desarrollo". Elementos que fueron definidos con posterioridad a la confección del documento - Especificación de Requerimientos de Software (ERS) – (versión borrador) analizado por esa unidad de auditoría"*.

Durante la entrevista de cierre llevada a cabo el 29 de abril de 2019, el Departamento Desarrollo de Sistemas de Servicios y Asistencia al Contribuyente (DI SRSS) y el Departamento Homologación de Sistemas de Recaudación, Seguridad Social y Servicios (DI SRSS) señalaron *"…estar de acuerdo con lo observado y procederán a analizar la documentación y los procesos llevados a cabo a fin de determinar las razones que permitieron la mencionada inconsistencia. Plazo estimado 30 días hábiles"*.

Por su parte, el Departamento Certificación de la Calidad de los Sistemas (DI ECCS) manifestó *"… estar de acuerdo con lo observado, se comprometen emitir normativa al respecto, a fin de regularizar la situación mencionada. Plazo estimado 30 días hábiles"*.

Causa

Falta de apego a la normativa vigente.

Incumplimiento de las misiones y funciones de las áreas involucradas.

Efecto

La falta de control de implementación de roles y perfiles en la Plataforma RDIC podría redundar en el acceso indebido a información sensible del personal del Organismo, poniendo en riesgo la confidencialidad de la información.

Potencial filtración de información sensible y confidencial del personal perteneciente del Organismo.

Recomendación

Se recomienda realizar y formalizar una adecuada definición de roles y perfiles y ajustar con celeridad la asignación de cada uno de ellos a los usuarios de la Plataforma RDIC.

Al mismo tiempo, se recomienda establecer un control periódico de asignación de roles y perfiles para la Plataforma RDIC, estableciendo un procedimiento de revalidación y depuración periódica de usuarios.

Plan de acción

Área Responsable con Competencia	Fecha prevista
Dirección de Integridad Institucional Departamento Desarrollo de Sistemas de Servicios y Asistencia al Contribuyente (DI SRSS) Departamento Homologación de Sistemas de Recaudación, Seguridad Social y Servicios (DI SRSS) Dirección de Tecnología y Arquitectura de los Sistemas (SDG SIT)	

Opinión/Plan de Acción del Auditado/Responsable con Competencia

La Dirección de Tecnología y Arquitectura de los Sistemas (SDG SIT), mediante correo electrónico del 14/05/2020, manifestó: *"Esta Dirección entiende que la esencia de la recomendación vertida por esa Unidad de Auditoría Interna no es de su entera competencia. No obstante, sin perjuicio a lo ya aclarado, toma conocimiento de la observación que le da origen"*.

La Dirección de Sistemas de Recaudación, Seguridad Social y Servicios (SDG SIT), mediante correo electrónico del 14/05/2020, manifestó: *"[…] Se elaboró una nueva versión del documento de especificación de requerimientos (ERS), al que se le incorporó la especificación de los ROLES implementados en el sistema junto con las transacciones que cada rol puede solicitar. Es oportuno aclarar que el documento anterior solamente mencionaba los "Actores" del sistema, como unidades lógicas para el entendimiento del requerimiento y no hacía referencia a la implementación concreta del mismo en la Consola de Gestión de Usuario. Si bien, el documento ERS es un detalle de requerimientos funcionales se incorporó a este documento un apartado con un detalle de los roles físicos del sistema implementados en la Consola de Gestión de Usuario. Por último, es el área definidora quien debe, según propios criterios, generar las reglas específicas en la misma Consola de Gestión de Usuarios, para determinar las personas que podrán solicitar cada rol"*.

La Dirección de Integridad Institucional, mediante el documento "Plan de Remediación: acciones mitigantes de riesgos residuales" adjunto al correo electrónico N° 131/2019 del 19/11/2019, manifestó: *"En cuanto a los roles y perfiles asignados respecto de la plataforma RDIC, que los mismos resultan correctos desde el punto de vista del uso de la herramienta. No obstante ello, y en vías de otorgar una solución a las observaciones planteadas, esta Dirección se comprometió a adecuar y formalizar la definición de los roles y perfiles, ajustando la asignación de cada uno de ellos a los usuarios de la plataforma RDIC. Consecuentemente, con el objetivo de atender los aspectos planteados por el Servicio de Auditoría, se adecuó el documento de "Especificaciones de Requerimientos de Software"*. Asimismo, mediante correo electrónico del 08/05/2020, manifestó: *"En tal sentido, corresponde reiterar los términos vertidos en el referido correo del 19/11, en donde se ratificó la nota de respuesta al Informe Preliminar sobre las medidas de seguridad del contexto y de infraestructura adoptadas por esta Dirección para la implementación de la plataforma RDIC, indicando que dichas cuestiones se encontraban cumplimentadas en su totalidad"*.

Opinión de Auditoría Interna

En función de lo manifestado por la ex Dirección de Integridad Institucional, por la Dirección de Sistemas de Recaudación, Seguridad Social y Servicios (SDG SIT) y del análisis realizado sobre la documentación de soporte remitida, esta Unidad de Auditoría comprobó que, si bien se ha formalizado la definición de roles y perfiles de la plataforma "RDIC – Administrador" en el entregable *"Especificación de Requerimientos de Software"*, el mismo no define ni formaliza el rol de "Carga DDJJ" en el sistema, así como tampoco determina a qué usuarios deben asignarse cada uno de los roles. Dicha asignación solamente puede inferirse vagamente en función de las especificaciones funcionales de cada actor. Esta situación dificulta la posibilidad de ejecutar un proceso de reválida de usuarios en la Plataforma RDIC.

En virtud de lo expuesto, teniendo en cuenta que mediante la Disposición N.° 140/2020 (AFIP) fue derogada la Disposición N.°

353/2017 (AFIP) – "Régimen Declarativo de Información Confidencial (RDIC)", en caso de no ser discontinuada la herramienta RDIC, se mantiene la recomendación oportunamente remitida y se refuerza la necesidad de que la documentación de Especificación de Requerimiento de Software (ERS) contenga en detalle los roles disponibles y la asignación correspondiente según puestos de trabajo.

Criticidad del Riesgo Residual					Efectividad del Control Interno					Estado de la observación
Ext	Alt	Mod	Baj	Mín	Def/In	Reg	MRe	Bue	Ópt	Con acción correctiva informada

Unidad auditable y Normativa aplicable

Tecnología de la Información – Entrega y Soporte – Garantizar la Seguridad

INSUMO	PROCESO	PRODUCTO
Arquitectura de la Información. Clasificación de Datos Asignados. Estándares de Tecnología. Evaluación de Riesgo. Especificaciones de Aplicaciones de Controles de Seguridad. Acuerdos de Nivel de Operación (OLAs).	El presente proceso tiene por finalidad mantener la integridad de la información y proteger los activos de TI e incluye el establecimiento y mantenimiento de roles y responsables de seguridad, políticas, estándares y procedimientos de TI, así como la realización de monitoreo de seguridad y pruebas periódicas, las que darán como resultado la implementación de acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Si bien es un proceso dinámico que, en cuanto a responsabilidades atraviesa prácticamente toda la estructura del Organismo, podemos decir que comienza con el relevamiento de los requerimientos de seguridad, de las vulnerabilidades y amenazas a la que están expuestos los recursos de TI (aplicaciones, información, infraestructura y personas) y con la administración estandarizada de identidades de usuarios y autorizaciones, para finalizar con la conducción en forma adecuada y oportuna de dichas vulnerabilidades.	Definición de Incidentes de Seguridad. Requerimientos de Capacitación para la Concientización Sobre Seguridad de TI. Reportes de Desempeño del Proceso. Implementación de Cambios en Materia de Seguridad, Amenazas y Vulnerabilidades de Seguridad. Políticas y Planes de Seguridad de TI.

Riesgos relevantes	1. Ciclo de vida de la aplicación incompleto: Cumplimiento parcial del Ciclo de Vida de la Aplicación, comprometiendo la seguridad de la misma. 2. Definición y asignación de roles y perfiles insegura: Falencias en la definición y/o asignación de roles y perfiles de usuarios de la aplicación, que podrían comprometer la seguridad de la misma. 3. Imposibilidad de reconstruir trazas informáticas: Imposibilidad de reconstruir cronológicamente sucesos informáticos (borrado, lectura y modificaciones de registros; identificando recursos informáticos físicos utilizados; horarios de ejecuciones; aplicativos/herramientas; etc.), que se corresponda con la interacción de un usuario con un sistema o de este último con cualquier otro. 4. Arquitectura de información no homologada: La presencia de una arquitectura de información no homologada y que no responde a un conjunto de estándares prefijados (políticas de calidad aprobadas) dificulta su correcta administración.
Controles asociados auditados (*)	1.1. Instrucciones, normas y procedimientos formalizados: Existencia de instrucciones, normas y procedimientos que establezcan las tareas que deben llevarse a cabo en el Ciclo de Vida de la Aplicación, y garanticen su seguridad. 1.2. Calidad de gestión: Existencia de evidencia acerca del grado de ajuste de las tareas realizadas a las instrucciones, normas y procedimientos formalizados. 2.1. Existencia y coherencia en la definición y asignación de roles y perfiles: Es el mecanismo de control de autorización de usuario, en donde, a cada usuario del sistema se le otorga un perfil de acceso en correspondencia con las labores que desempeña dentro del Organismo. Los perfiles de accesos distinguen jerarquías ejecutivas, operativas y administrativas. Consecuentemente, cada perfil posee uno o más roles en forma correspondiente a las acciones que puede realizar el usuario en el sistema. Finalmente, los privilegios son las habilitaciones de acciones dentro de cada rol definido. 3.1. Pistas de auditoría: Las pistas de auditoría brindan un mapa para trazar por segunda vez el flujo de una transacción. Permite recrear el flujo real de transacciones a partir del punto en que se originan hasta su ubicación en un archivo o repositorio. Se registra desde quien inició la transacción, la hora y la fecha de ingreso, el tipo de ingreso, qué campos de información contenía y qué archivos actualizó. La registración cronológica de los sucesos informáticos relacionados a cada usuario permite no sólo el deslinde de responsabilidades sino también permite reconstruir los hechos ante un posible delito,

	fraude, etcétera. 4.1. Arquitectura de seguridad: Revisión y análisis de la información de la arquitectura definida, a fin de evaluar la seguridad de la misma. 4.2. Monitoreo de la arquitectura de seguridad: Existe evidencia de los controles de monitoreo realizados a fin de garantizar la seguridad de la arquitectura de información.
Objetivos de Auditoría (**)	1.1.1. Verificar la existencia de políticas, normas, procedimientos, controles, y tareas que garanticen la seguridad del Ciclo de Vida del Desarrollo. **(AP)** 1.2.1. Verificar que se haya realizado el adecuado monitoreo a lo largo del Ciclo de Vida del Desarrollo de la Plataforma RDIC. **(AP)** 1.2.2. Verificar que se haya realizado el control y aceptación del resultado final en el ambiente productivo por parte del área definidora. **(1, A)** 2.1.1. Realizar un análisis de módulos, roles y perfiles asignados a los usuarios intervinientes en el proceso, a fin de corroborar la coherencia en la definición y asignación de roles y perfiles. **(2, 3)** 3.1.1. Verificar la existencia de políticas, normas y procedimientos debidamente formalizados, respecto de la registración, almacenamiento y control de las pistas de auditoría (logs). **(AP)** 3.1.2. Verificar la existencia de un proceso automático de la Plataforma RDIC que registre las pistas de auditoría (logs) de acuerdo con los procedimientos internos o con las mejores prácticas. **(AP)** 4.1.1. Realizar una revisión de la seguridad de la arquitectura sobre la cual se encuentra montada la Plataforma RDIC, respecto del Sistema Operativo. **(AP)** 4.1.2. Realizar una revisión de la seguridad de la arquitectura sobre la cual se encuentra montada la Plataforma RDIC, respecto del Sistema de Gestión de Base de Datos. **(AP)** 4.2.1. Realizar una revisión de la seguridad de la arquitectura sobre la cual se encuentra montada la Plataforma RDIC, respecto del Sistema Operativo. **(AP)** 4.2.2. Realizar una revisión de la seguridad de la arquitectura sobre la cual se encuentra montada la Plataforma RDIC, respecto del Sistema de Gestión de Base de Datos. **(AP)**

(*) Se enumeran únicamente los controles seleccionados para ser auditados durante las tareas de campo, considerando su relevancia respecto de la criticidad de los riesgos que pretenden mitigar.

(**) Referencias: (A): Alcance - (AP): Aclaraciones Previas - (S/O): Sin observación - (N.°): N.° de Observación correspondiente.

Normativa aplicable

	Norma	Vigencia
Normativa general	**Decreto N.° 378/2005** - Plan Nacional de Gobierno Electrónico y Planes Sectoriales.	28/04/2005
	Resolución N.° 290/2019 (SGN) - Reglamento para el Funcionamiento del Comité de Control Interno.	20/08/2019
	Resolución N.° 172/2014 (SGN) - Normas Generales de Control Interno para el Sector Público.	28/11/2014
	Resolución N.° 36/2011 (SGN) - Aprobación del Programa de Fortalecimiento del Sistema de Control Interno.	01/04/2011
	Resolución N.° 48/2005 (SGN) - Normas Control Interno Tecnología Información.	23/05/2005
	Resolución N.° 45/2003 (SGN) - Papeles de trabajo.	12/05/2003
	Resolución N.° 152/2002 (SGN) - Normas de Auditoría Interna Gubernamental.	17/10/2002
	Disposición N.° 29/2019 (AFIP) - Política de Seguridad de la Información. Disposición N.° 76/05 (AFIP). Su sustitución.	05/02/2019
	Disposición N.° 07/2019 (SDG AUI) - Manual de Auditoría – Versión 6.2.	20/05/2019
	Instrucción General N.° 01/2016 (AFIP) - Servicio de auditoría interna. Su alcance, tratamiento a observar por las unidades de estructura dependientes de la AFIP.	01/03/2016

	Instrucción General N.° 01/2016 (SDG AUI) – Instrucción General N.° 01/2016 (AFIP). Su reglamentación por la SDG AUI, conforme Punto XI – Disposiciones Generales., Apartado 7.	09/03/2016
	Instrucción General N.° 03/2011 (SDG SIT) - Norma para la administración de accesos a los sistemas informáticos de la AFIP.	23/08/2011

	Norma	Vigencia
Normativa específica	**Disposición N.° 353/2017** (**AFIP)** - "Declaración jurada informativa – Ética en la función pública – Código de ética".	21/11/2017
	Instrucción General N.° 01/2019 (SDG SIT) - Pautas para el Desarrollo, Mantenimiento y Discontinuidad de los Sistemas Informáticos de la AFIP.	04/09/2019
	Instrucción General N.° 2/2018 (AFIP) - "Funcionarios de la DGI – Régimen Declarativo de Información Confidencial - RDIC - ".	27/07/2018
	Instrucción General N.° 01/2018 (**AFIP**) - "Ética de la función pública – Régimen Declarativo de Información Confidencial – RDIC –".	21/06/2018
	Instrucción General N.° 01/2017 (AFIP) -" Ética de la función pública – Régimen Declarativo de Información Confidencial – RDIC –".	15/12/2017
	ISACA Marco de Referencia COBIT 2019 - Objetivos de gobierno y gestión.	01/01/2019
	NIST - Publicación 800-53, "Security and Privacy Controls for Information Systems and Organizations", del "National Institute of Standards and Technology" (NIST).	01/08/2017

Datos Referenciales

	Cargo	(Título) Apellido y Nombre
Equipo de Auditoría	Subdirectora General de Auditoría Interna	C.P. CAMILLETTI, Gabriela Noemí
	Coordinador y Supervisor de la Dirección de Auditoría de Procesos Centrales	Lic. GOGLIORMELLA, Christian Eduardo
	Jefa (Int.) de Departamento Auditoría de Tecnología de la Información	Ing. PACINI, Luz María
	Supervisor (a/c)	Ing. DE PERINI, Carlos María
	Auditores	Sr. MIGUEZ, Matías Luciano Sr. COHEN SEMAG, Guido

	Cargo	Durante las Tareas de Campo	Durante el Período Auditado
Área Auditada o Responsable (autoridades / jefaturas / responsables)	Subdirector General de Sistemas y Telecomunicaciones	Lic. DUNAYEVICH, Julián Lic. SPETTOLI, Fernando Rubén	Lic. SPETTOLI, Fernando Rubén Lic. ROUGET, Sandra Lía C.P. SOSA, Néstor Abelardo
	Director de Seguridad de la Información	Ing. PASSERINI, Pablo Nicolás Ing. NAVARRO, Pablo Mariano	Ing. NAVARRO, Pablo Mariano Lic. SPETTOLI, Fernando Rubén
	Director de Integridad Institucional	DARSAUT, Ariel Horacio	Lic. RUSSO, Marcos José
	Director de Tecnología y Arquitectura de los Sistemas (SDG SIT)	Ing. LAGOSTENA, Juan Pablo A. S. MIRANDA, Carlos Alejandro	-
	Director de Sistemas de Recaudación, Seguridad Social y Servicios (SDG SIT)	Lic. PALACIOS, Claudio Santiago	Lic. PALACIOS, Claudio Santiago
	Director de Estandarización y Certificación de la Calidad de los Servicios y Procesos (SDG SIT)	A.S. MIRANDA, Carlos Alejandro	A.S. SALVIA, Adriana Cristina
	Director de Operaciones Informáticas (SDG SIT)	Ing. DEMARTINI, Diego Lic. LEIS, Fabián Gustavo A.S. IANNICELLI, Marcelo Eugenio	A.S. IANNICELLI, Marcelo Eugenio A.S. TRAVERSO, Ivanoe
	Jefe de Departamento Arquitectura de los sistemas (DI TEAS)	Lic. SCASSO, Marcelo Ing. ZAFFARANO, Sebastián Pascual	-
	Jefe de Departamento Seguridad Informática (SDG SIT)	Lic. OHYAMA, Miguel Ulises	Sr. PAZO, Gastón Horacio
	Jefe de Departamento Desarrollo de Sistemas de Servicios y Asistencia al Contribuyente (DI SRSS) [Vigencia 25/07/2018 - Presente]	Ing. MAJCHRZAK, Esteban Enrique	Ing. MAJCHRZAK, Esteban Enrique
	Jefe de Departamento Homologación de Sistemas de Recaudación, Seguridad Social y Servicios (DI SRSS) [25/07/2018 - Presente] / Jefe de Departamento Prueba y Homologación de Sistemas de los Recursos Seguridad Social y Procesos Centrales (DI PHSI) [Vigencia 01/12/2017 - 24/07/2018]	Sr. MACEIRAS, Gonzalo	Sr. MACEIRAS, Gonzalo
	Jefe de Departamento Calidad de los Sistemas (DI TEAS) [Vigencia	Lic. JORDAN, Jaqueline del Valle	Lic. JORDAN, Jaqueline del Valle

	05/08/2019 – Presente] / Jefe de Departamento Certificación de la Calidad de los Sistemas (DI ECCS) [Vigencia 04/12/2017 - 05/08/2019]		
	Jefe de Departamento Administración de Hardware y Software de Base (DI OPEI) [Vigencia 25/07/2018 - Presente]	A.C. RELATS DE DALMASES, Jorge	A.C. RELATS DE DALMASES, Jorge
	Jefe de Departamento Soporte Técnico (DI OPEI) [Vigencia 01/12/2017 - 24/07/2018] / Jefe de Departamento Soporte Técnico (DI OPIN) [Vigencia 04/04/2016 - 30/11/2017]	-	A.C. RELATS DE DALMASES, Jorge

TAREAS REALIZADAS:

Descripción	Fecha desde/hasta
Se comunicó el inicio del seguimiento del presente cargo de auditoría, mediante el Correo Oficial N° 91/2020 y el Correo Oficial N° 92/2020 a la Subdirección General de Sistemas y Telecomunicaciones y la Dirección de Integridad Institucional respectivamente.	04/05/2020
Se analizaron las respuestas al Informe de Auditoría Interna junto con la documentación soporte recibida por parte de la Dirección de Integridad Institucional.	08/05/2020
Se analizaron las respuestas al Informe de Auditoría Interna junto con la documentación soporte recibida por parte de la Subdirección General de Sistemas y Telecomunicaciones.	14/05/2020
Se confeccionó la planilla con las actividades de control para establecer los procedimientos que se deberán llevar a cabo en el seguimiento del presente cargo de auditoría.	11/06/2020
Se llevó a cabo la revisión y el análisis de la Instrucción General N.° 01/2019 (SDG SIT) – "Pautas para el Desarrollo, Mantenimiento y Discontinuidad de los Sistemas Informáticos de la AFIP" en función de las respuestas recibidas por las áreas auditadas.	16/06/2020
Se elaboraron los papeles de trabajo de auditoría cuyo contenido comprende el objetivo, análisis y conclusión abordada a partir de la información y documentación soporte recibida.	18/06/2020
Se compararon los roles y perfiles definidos en la Especificación de Requerimientos de Software, remitida por la Dirección de Integridad Institucional, con los roles asignados a los usuarios de la Plataforma RDIC.	23/06/2020
Se comparó cada uno de los roles asignados a los usuarios de los agentes que utilizan la plataforma RDIC, con el esquema de reglas establecido en dicha plataforma.	23/06/2020
Se comparó cada uno de los roles asignados a los usuarios de los agentes que utilizan la plataforma RDIC, con el esquema de reglas establecido en dicha plataforma.	23/06/2020
Se compararon los roles y perfiles definidos en la Especificación de Requerimientos de Software, remitida por la Dirección de Integridad Institucional, con los roles asignados a los usuarios de la Plataforma RDIC.	31/05/2021
Se solicitaron los logs de acceso a la herramienta.	11/06/2021
Se analizaron los logs de accesos para verificar si se produjeron ingresos a la herramienta en forma posterior a la fecha de derogación de uso.	07/07/2021

REFERENCIAS DEL INFORME

En el presente informe se interpreta de la siguiente manera los conceptos que seguidamente se detallan:

1. La criticidad del Riesgo Residual de las observaciones:

Ext	Extrema
Alt	Alta
Mod	Moderada
Baj	Baja
Mín	Mínima

2. La Efectividad del Control Interno evaluado:

Def/In	Deficiente o Inexistente
Reg	Regular
MRe	Más que Regular
Bue	Bueno
Ópt	Óptimo

Anexo C

Comunicación con el auditado y otras áreas con competencia

A continuación, se presenta un detalle de la comunicación establecida entre la comisión auditora y los distintos responsables de las áreas involucradas:

COMUNICACIONES ENVIADAS

Área / Fecha	Comunicación	Asunto	¿El área auditada respondió? (SI/NO)
SUBDIRECCIÓN GENERAL DE SISTEMAS Y TELECOMUNICACIONES			
05/07/2021	Correo electrónico S/N	RE: CSI 11/2020 - Análisis de Incidentes por Accesos a los Sistemas -Solicitud de Información	Si
11/06/2021	Correo electrónico S/N	Re: CSI 11/2020 - Análisis de Incidentes por Accesos a los Sistemas -Solicitud de Información	Si
07/06/2021	Correo electrónico S/N	CSI 11/2020 - Análisis de Incidentes por Accesos a los Sistemas -Solicitud de Información	Si
31/05/2021	Correo electrónico S/N	Consulta sobre áreas responsables de desarrollo	Si
04/05/2020	Correo Oficial N° 91/2020 (DI AUPC)	Comunicación de Inicio de Seguimiento - CSI 15/2019 - Entrega y Soporte -Análisis Manejo de Información en Plataforma RDIC	Si
28/06/2019	IF-2019-00187547-AFIP-DIAUPL#SDGAUI	Remisión del Informe de Auditoría Interna	Si
DIRECCIÓN DE INTEGRIDAD INSTITUCIONAL			
04/05/2020	Correo Oficial N° 92/2020 (DI AUPC)	Comunicación de Inicio de Seguimiento - CSI 15/2019 - Entrega y Soporte -Análisis Manejo de Información en Plataforma RDIC	Si
28/06/2019	IF-2019-00187541-AFIP-DIAUPL#SDGAUI	Remisión del Informe de Auditoría Interna	Si

COMUNICACIONES RECIBIDAS

Área / Fecha	Comunicación	Asunto
SUBDIRECCIÓN GENERAL DE SISTEMAS Y TELECOMUNICACIONES		
05/07/2021	Correo electrónico S/N	RE: CSI 11/2020 - Análisis de Incidentes por Accesos a los Sistemas -Solicitud de Información
15/06/2021	Correo electrónico S/N	Re: CSI 11/2020 - Análisis de Incidentes por Accesos a los Sistemas -Solicitud de Información
07/06/2021	Correo electrónico S/N	CSI 11/2020 - Análisis de Incidentes por Accesos a los Sistemas -Solicitud de Información
31/05/2021	Correo electrónico S/N	Consulta sobre áreas responsables de desarrollo
14/05/2020	Correo electrónico S/N	Respuestas por parte de DI TEAS y DI SRSS al Informe de Auditoría Interna
14/08/2019	IF-2019-00260026-AFIP-SDGSIT con Nota N° 39/2019 y Nota N° 186/2019	Respuestas por parte de DI TEAS y DI SRSS al Informe de Auditoría Interna
DIRECCIÓN DE INTEGRIDAD INSTITUCIONAL		
08/05/2020	Correo Oficial N° 46/2020	Respuesta por parte de DI INIT al Informe de Auditoría Interna
04/05/2020	Correo electrónico S/N	Solicitud de reenvío del Informe de Auditoría Interna

Área / Fecha	Comunicación	Asunto
19/11/2019	Correo electrónico N° 131/2019	Plan de remediación - Acciones mitigantes de riesgos residuales

Anexo D

Detalles técnicos de las observaciones / recomendaciones

Por las características del presente informe, no corresponde la exhibición del detalle enunciado en el Informe.

Administración Federal de Ingresos Públicos
2021 - AÑO DE HOMENAJE AL PREMIO NOBEL DE MEDICINA DR. CÉSAR MILSTEIN

Hoja Adicional de Firmas
Informe gráfico firma conjunta

Número: IF-2021-00855831-AFIP-SDGAUI

CIUDAD DE BUENOS AIRES
Lunes 2 de Agosto de 2021

Referencia: ISF CSI 15-2019 - RDIC - SIGEN

El documento fue importado por el sistema GEDO con un total de 22 pagina/s.

Digitally signed by GDE AFIP
DN: cn=GDE AFIP, c=AR, o=ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS, ou=SUBDIRECCION GENERAL DE COORDINACION TECNICO INSTITUCIONAL, serialNumber=CUIT 33693450239
Date: 2021.07.30 14:29:19 -03'00'

COHEN SEMAG, GUIDO
Auditor
Departamento Auditoría de Tecnología de la Información
Administración Federal de Ingresos Públicos

Digitally signed by GDE AFIP
DN: cn=GDE AFIP, c=AR, o=ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS, ou=SUBDIRECCION GENERAL DE COORDINACION TECNICO INSTITUCIONAL, serialNumber=CUIT 33693450239
Date: 2021.07.30 14:33:50 -03'00'

MIGUEZ, MATIAS LUCIANO
Auditor
Departamento Auditoría de Tecnología de la Información
Administración Federal de Ingresos Públicos

Digitally signed by GDE AFIP
DN: cn=GDE AFIP, c=AR, o=ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS, ou=SUBDIRECCION GENERAL DE COORDINACION TECNICO INSTITUCIONAL, serialNumber=CUIT 33693450239
Date: 2021.07.30 15:02:53 -03'00'

DE PERINI, CARLOS MARIA
Supervisor
Departamento Auditoría de Tecnología de la Información
Administración Federal de Ingresos Públicos

Digitally signed by GDE AFIP
DN: cn=GDE AFIP, c=AR, o=ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS, ou=SUBDIRECCION GENERAL DE COORDINACION TECNICO INSTITUCIONAL, serialNumber=CUIT 33693450239
Date: 2021.07.30 16:26:04 -03'00'

PACINI, LUZ MARIA
Jefa de Departamento
Departamento Auditoría de Tecnología de la Información
Administración Federal de Ingresos Públicos

Digitally signed by GDE AFIP
DN: cn=GDE AFIP, c=AR, o=ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS, ou=SUBDIRECCION GENERAL DE COORDINACION TECNICO INSTITUCIONAL, serialNumber=CUIT 33693450239
Date: 2021.07.30 19:08:37 -03'00'

GOGLIORMELLA, CHRISTIAN EDUARDO
Coordinador y Supervisor
Dirección de Auditoría de Procesos Centrales
Administración Federal de Ingresos Públicos

Digitally signed by GDE AFIP
DN: cn=GDE AFIP, c=AR, o=ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS, ou=SUBDIRECCION GENERAL DE COORDINACION TECNICO INSTITUCIONAL, serialNumber=CUIT 33693450239
Date: 2021.08.02 13:11:12 -03'00'

CAMILLETTI, GABRIELA NOEMI
Subdirectora General
Subdirección General de Auditoría Interna
Administración Federal de Ingresos Públicos

Digitally signed by GDE AFIP
DN: cn=GDE AFIP, c=AR, o=ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS, ou=SUBDIRECCION GENERAL DE COORDINACION TECNICO INSTITUCIONAL, serialNumber=CUIT 33693450239
Date: 2021.08.02 13:11:14 -03'00'