ESPECIALIZACIÓN EN AUDITORÍA INTERNA GUBERNAMENTAL

FACULTAD DE CIENCIAS ECONÓMICAS
UNIVERSIDAD NACIONAL DE LA PLATA

TRABAJO INTEGRADOR FINAL

Iniciativas innovadoras para el fortalecimiento del sistema de control interno

Elaboración de Legajos Digitales para las Unidades de Auditoría Interna

AUTOR: [GRASSO, NÉSTOR GUSTAVO]

DIRECTOR: [RUMITTI, CARLOS]

CO-DIRECTOR: [CÓCCARO, ANA]

[OCTUBRE 2021]

1. ÍNDICE

Tabla de contenido

2. DESCRIPCIÓN DEL TEMA A ABORDAR

El proyecto partirá de una problemática actual a partir del estudio, análisis y descripción de la situación de diferentes Unidades de Auditoría Interna (UAI) respecto de la gestión de la documentación de auditoría que soporta el desarrollo de las actividades de control y se intentará brindar una solución superadora con la incorporación de herramientas tecnológicas.

Cabe comentar, que fui uno de los precursores de la despapelización en la Unidad de Auditoría Interna donde me desempeño, presentando oportunamente una propuesta a la SIGEN de un procedimiento para suplantar el legajo físico de auditoría por el legajo digital, el cual fue aprobado y luego refrendado por una Resolución Ministerial.

Por otra parte, la participación en la Especialización de Auditoría Gubernamental me dio la posibilidad de interiorizarme sobre cómo se maneja el resto de las UAI, habiendo notado que muchas todavía siguen utilizando legajos en papel en mayor o menor medida y las que emplean legajos digitales en muchos casos carecen de una metodología adecuada.

3. FUNDAMENTO DEL TEMA, DELIMITACIÓN Y APORTE

Resulta necesario reformular el sistema de gestión y administración de la documentación que sustenta la ejecución de los diferentes proyectos de auditoría llevados a cabo por las Unidades de Auditoría Interna, a fin de incorporar las ventajas reales que ofrecen las Nuevas Tecnologías de la Información y Comunicación.

Por ello, es de suma importancia avanzar en el análisis y elaboración de una metodología para la digitalización de la documentación de auditoría y gestionarla de manera segura, con el objetivo de minimizar la utilización y almacenamiento de la información en soporte papel, manteniendo la confidencialidad, disponibilidad e integridad de la información.

4. OBJETIVOS PROPUESTOS (GENERALES – ESPECÍFICOS)

El objetivo general del trabajo radica en proponer una metodología superadora para la elaboración de legajos digitales de auditoría, incorporando, para tal fin, las ventajas que ofrecen las Nuevas Tecnologías de la Información y Comunicación.

Para ello, se establecieron una serie de objetivos específicos a saber:

- Llevar a cabo un relevamiento del contexto actual en distintas Unidades de Auditoría Interna de la Administración Pública Nacional respecto de la metodología utilizada para la gestión de la documentación de auditoría.
- A partir del resultado de dicho relevamiento, identificar problemas comunes y analizar posibles mejoras.
- Proponer una estructura homogénea para la gestión de los legajos digitales y elaborar un sistema eficiente de referenciación de dichos legajos.
- Propiciar medidas tendientes a garantizar la confidencialidad, integridad e Inviolabilidad de la información contenida en los legajos digitales.

5. MARCO TEÓRICO

I. SISTEMA DE CONTROL INTERNO EN EL SECTOR PÚBLICO NACIONAL

La ley 24.156 es la que establece y regula la administración financiera y los sistemas de control del sector público nacional.

"La administración financiera comprende el conjunto de sistemas, órganos, normas y procedimientos administrativos que hacen posible la obtención de los recursos públicos y su aplicación para el cumplimiento de los objetivos del Estado" (Ley 24.156, art 2º).

Por su parte, "los sistemas de control comprenden las estructuras de control interno y externo del sector público nacional y el régimen de responsabilidad que estipula y está asentado en la obligación de los funcionarios de rendir cuentas de su gestión" (Ley 24.156, art 3º).

Uno de los objetivos de la Ley es el de establecer la implantación y mantenimiento de "un eficiente y eficaz sistema de control interno normativo, financiero, económico y de

gestión sobre sus propias operaciones, comprendiendo la práctica del control previo y posterior y de la auditoria interna" (Ley 24.156, art 4º).

Adicionalmente, establece que "La Sindicatura General de la Nación y la Auditoría General de la Nación serán los órganos rectores de los sistemas de control interno y externo, respectivamente" (Ley 24.156, art 7º).

Las disposiciones de la Ley son de aplicación en todo el Sector Público Nacional, el que a tal efecto está integrado por (Ley 24.156, art 8º):

> a) Administración nacional, conformada por la administración central y los organismos descentralizados, comprendiendo en estos últimos a las instituciones de seguridad social;
>
> b) Empresas y sociedades del Estado que abarca a las empresas del Estado, las sociedades del Estado, las sociedades anónimas con participación estatal mayoritaria, las sociedades de economía mixta y todas aquellas otras organizaciones empresariales donde el Estado tenga participación mayoritaria en el capital o en la formación de las decisiones societarias.

Con respecto a la conformación del sistema de control la Ley establece que:

> El sistema de control interno queda conformado por la Sindicatura General de la Nación, órgano normativo, de supervisión y coordinación, y por las Unidades de Auditoría Interna que serán creadas en cada jurisdicción y en las entidades que dependan del Poder Ejecutivo Nacional. Estas unidades dependerán, jerárquicamente, de la autoridad superior de cada organismo y actuarán coordinadas técnicamente por la Sindicatura General. (Ley 24.156, art 100º)

Con relación a la función de la Auditoria Interna la Ley determina que:

> La Auditoría Interna es un servicio a toda la organización y consiste en un examen posterior de las actividades financieras y administrativas de las entidades a que hace referencia esta ley, realizada por los auditores integrantes de las unidades de auditoria interna. Las funciones y actividades de los auditores internos deberán mantenerse desligadas de las operaciones sujetas a su examen. (Ley 24.156, art 102º)

II. DOCUMENTACIÓN DE AUDITORÍA

En el marco de los lineamientos contenidos en el *Anexo IV del Manual de Control Interno Gubernamental de la Sindicatura General de la Nación*, referido a la confección de los Papeles de Trabajo, se definen los aspectos con relación al tratamiento documental de los Legajos Corrientes, referidos a la documentación respaldatoria de las tareas ejecutadas por las Unidades de Auditoría Interna del Sector Público Nacional.

Respecto de la importancia de su elaboración la norma establece que:

> Los papeles de trabajo constituyen las evidencias respaldatorias de todo trabajo de auditoría […] para el adecuado y eficiente desempeño del auditor, teniendo en cuenta la importancia que reviste la registración de las pruebas de auditoría realizadas, así como el conocimiento y comprensión del universo a auditar, sobre el cual se basan sus conclusiones. (SIGEN, Manual de Control Interno Gubernamental, pág. 160)

En tal sentido, respecto de su confección se menciona que:

> Los papeles de trabajo están constituidos por todos los formularios y documentos que contienen información obtenida y elaborada por el auditor, desde la etapa de planificación hasta el cierre de auditoría […] los cuales serán reservados en legajos preparados para tal fin. (SIGEN, Manual de Control Interno Gubernamental, pág. 160).

Adicionalmente, respecto de la relación de los papeles de trabajo con el informe de auditoría la norma señala que:

> Los papeles de trabajo son el nexo entre el trabajo de campo y el informe de auditoría y deberán contener la evidencia para apoyar las observaciones, conclusiones y recomendaciones del informe. En tal sentido deben exponer de modo indubitable la prueba reunida y las evidencias en que fundamentara los aspectos salientes de su informe. (SIGEN, Manual de Control Interno Gubernamental, pág. 160).

Finalmente, respecto del avance de la tecnología y su impacto en la labor de auditoría menciona lo siguiente:

> El avance creciente de los negocios y el progreso tecnológico representó la aparición de modernos medios como soporte de operaciones y en reemplazo de registros, disminuyendo o directamente eliminando elementos de papel. Por ello, la posibilidad de que los papeles de trabajo puedan estar integrados por elementos que no sean papel […] está limitada en principio a la circunstancia de que ya sea por sí mismo o por la existencia de otros elementos que le sirvan de soporte, resulten aptos para sustentar la evidencia que de ellos se pretenda obtener" (SIGEN, Manual de Control Interno Gubernamental, pág. 160).

II.1. DOCUMENTCIÓN EN FORMATO DIGITAL

A través de la Resolución 190/2015 la SIGEN aprobó una prueba piloto para la implementación de *Papeles de Trabajo Digitales*.

Al respecto, se menciona en dicha norma que "a partir de los avances tecnológicos, se hace propicio avanzar en un proceso de despapelización de los procedimientos administrativos, acorde con los objetivos que apuntan a reducir el impacto ambiental y afectar eficientemente los recursos" (SIGEN, Resolución 190, 2015).

Adicionalmente, respecto de la importancia de la utilización de tecnologías de la información, la norma señala que:

> Contar con documentos electrónicos en reemplazo del papel y orientados al uso de Tecnologías de la Información se torna de suma importancia, dada la función que ocupan actualmente estas herramientas en las labores cotidianas. Dicho reemplazo, requiere el uso de tecnologías tales como el documento electrónico, la firma digital y otras herramientas en materia de seguridad informática. (SIGEN, Resolución 190, 2015).

Cabe señalar, que la prueba piloto mencionada sólo se llevo a cabo oportunamente en algunas Unidades de Auditoría Interna, a partir de una invitación exclusiva por parte de la SIGEN, no haciéndose extensiva la implementación de la metodología al resto de las Unidades.

Desde 2015 a la fecha, no se ha avanzado sobre la temática a nivel normativo.

Es en este sentido, habiendo sido partícipe de dicha prueba piloto la Unidad de Auditoria donde presto funciones, es que entiendo resulta enriquecedor el aporte que pueda hacerle a la metodología propuesta a partir de la propia experiencia y el relevamiento de la problemática existente actualmente en el resto de la UAI sobre el particular.

6. METODOLOGÍA A EMPLEAR

El alcance del proyecto será de tipo **Descriptivo**, partiendo de una problemática actual se intentará, con la utilización de la tecnología, brindar soluciones para mejorarla y potenciarla.

Respecto del diseño de la investigación será de tipo **Cualitativa**, basada en un diseño **No experimental** que permita estudiar, examinar y describir la situación de las diferentes Unidades de Auditoria Interna respecto de la confección de sus legajos de auditoría.

7. RELEVAMIENTO DE LA SITUACIÓN ACTUAL

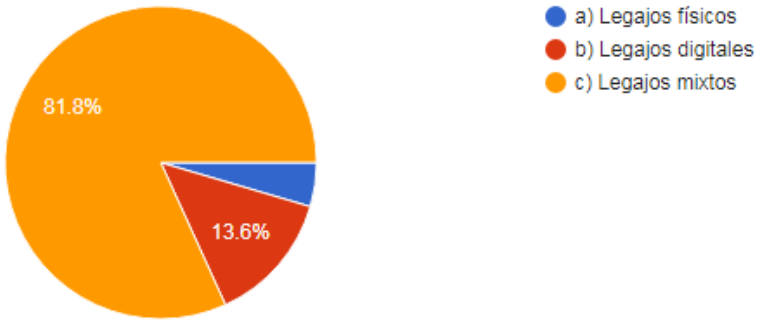
A fin de obtener un panorama de la situación actual en las que se encuentran las Unidades de Auditoría Interna respecto de la utilización de la tecnología en la administración de la documentación que sustenta los respectivos proyectos de auditoría llevados a cabo, se llevó a cabo un relevamiento a partir de la realización de una **encuesta** (ver ANEXO) sobre una muestra de 21 Unidades de Auditoría, a fin de determinar, entre otras cuestiones, lo siguiente:

- ✓ Cantidad de Unidades de Auditoría que aún mantiene su documentación en forma física.
- ✓ Cantidad de Unidades de Auditoría que mantienen duplicidad de información en la gestión de la documentación, elaborando legajos digitales y físicos sobre cada una de las auditorías realizadas.
- ✓ Cantidad de Unidades de Auditoría que, si bien trabajan con información digital, no poseen una metodología documentada y aprobada por autoridad competente para su conformación.

- ✓ Medidas de seguridad de la información aplicadas a los legajos digitales en la diferentes Unidades.
- ✓ Utilización de la firma digital a fin de darle integridad a los legajos.

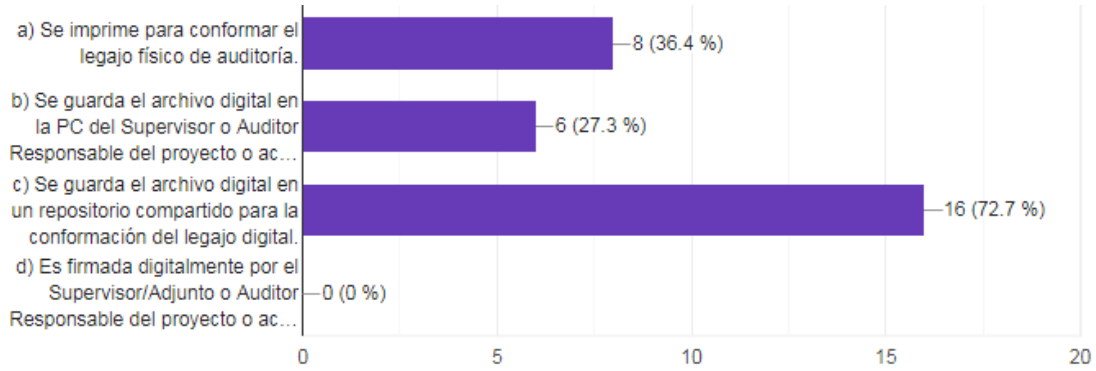
A continuación se exponen las preguntas efectuadas y el análisis de las respuestas obtenidas:

1) En la Unidad de Auditoría Interna donde se desempeña la documentación de auditoría resultante de la ejecución de los proyectos y actividades de auditoría se resguardan en:



Del gráfico que antecede se desprende que sólo el 13,6 % de las UAI encuestadas mantienen un sistema de legajos digitales únicamente. Asimismo, se evidencia que, en la mayoría de los casos, se llevan a cabo legajos mixtos para el resguardo documental resultante de la ejecución de los proyectos de auditoría, lo que puede repercutir negativamente en términos de homogeneidad, integridad, duplicidad de información y referenciación de estos legajos.

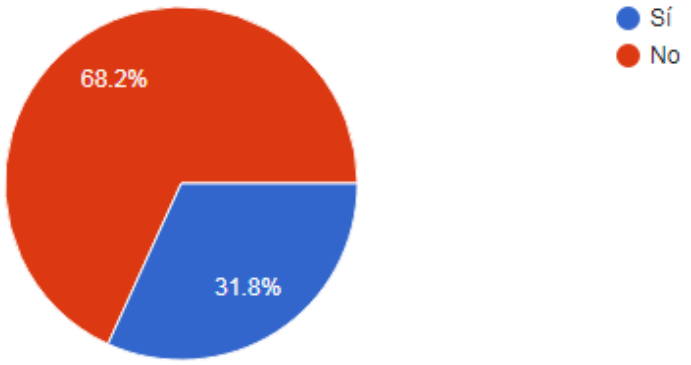
2) Si en el transcurso de una auditoría le remiten información digital como evidencia de algún procedimiento, que hacen con dicha evidencia?:



Como puede apreciarse en el gráfico, el 36,4 % de las UAI consultadas todavía mantienen la práctica de imprimir información obtenida para la conformación de los respectivos legajos físicos de auditoría, afectando la eficiencia de la labor desarrollada y generando un dispendio de recursos innecesarios tanto materiales como de espacio físico.

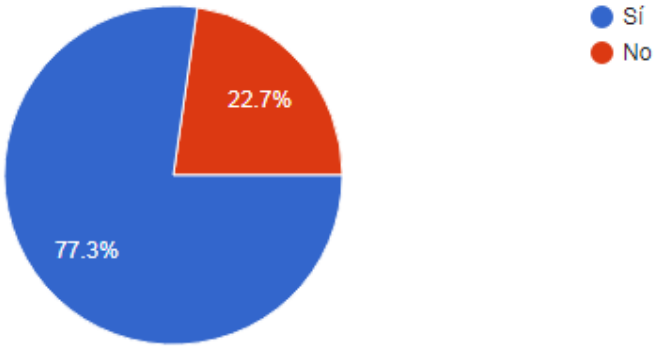
Asimismo, el 27,3 % de los encuestados informó que la información digital obtenida de los procedimientos de auditoría llevados a cabo son resguardados en la PC del Supervisor o Responsable del proyecto o actividad desarrollada. Tal situación genera un alto riesgo de pérdida de información dado que, generalmente, las PCs no forman parte de los procedimientos de salvaguarda de datos.

3) Posee la Unidad de Auditoría Interna un procedimiento para la elaboración de legajos digitales de auditoría que defina una estructura uniforme para su confección?



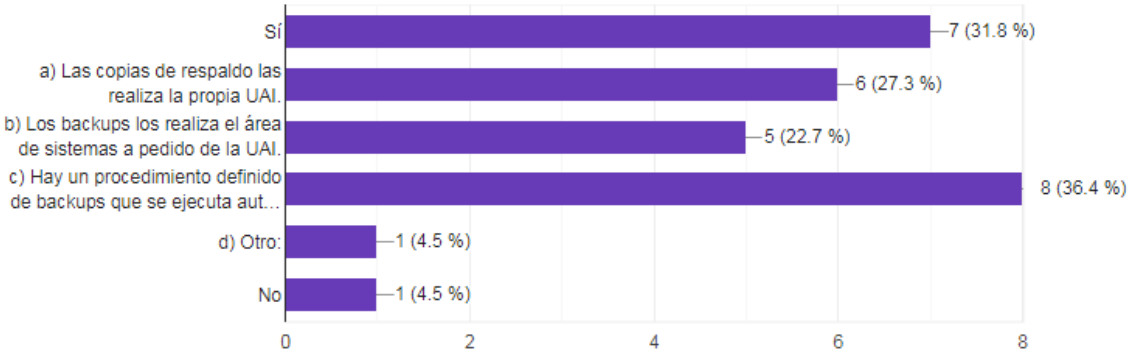
Como puede apreciarse en el gráfico que precede, el 68,2 % de las UAI consultadas no poseen un procedimiento documentado para la elaboración de legajos digitales que establezca, entre otras cuestiones, un esquema uniforme para la conformación de dichos legajos.

4) Posee la Unidad de Auditoría Interna un repositorio de acceso compartido por todos los agentes para el resguardo de información digital?



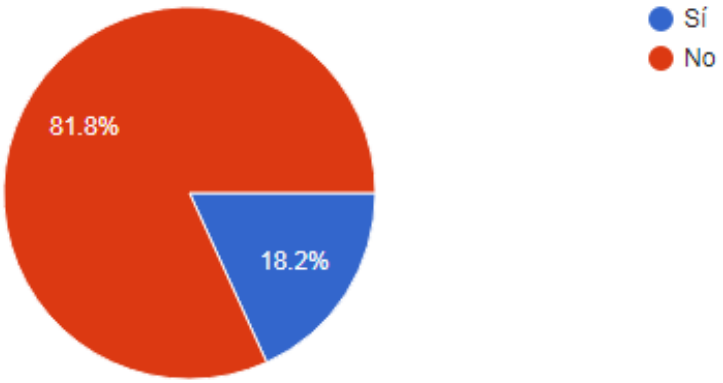
De los guarismos precedentes surge que el 22,7 % de las UAI no posee un espacio compartido para el resguardo de información digital, situación que repercute negativamente en la implementación de medidas de gestión de información centralizada.

5) Se llevan a cabo copias de resguardo de los legajos digitales?



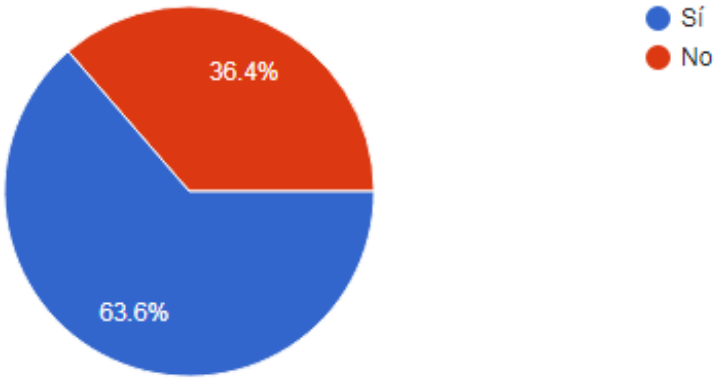
Del gráfico precedente surge que sólo el 36,4 % de las Unidades posee un procedimiento definido de resguardo de información que se ejecuta de manera automática. Tal situación denota un alto riesgo de pérdida de información ante un eventual siniestro.

7) Se lleva a cabo algún procedimiento para garantizar la inalterabilidad de los legajos digitales una vez culminada la auditoría?



Como puede advertirse, el 81,8 % de las Unidades de Auditoría consultadas carece de un procedimiento que garantice la inalterabilidad de la información una vez culminados los proyectos de auditoría y conformados los legajos correspondientes, generando un alto riesgo de pérdida de integridad de la información contenida en dichos legajos.

8) Poseen los legajos digitales algún mecanismo de referenciación interna que relacione, por ejemplo, las evidencias con los hallazgos detectados?



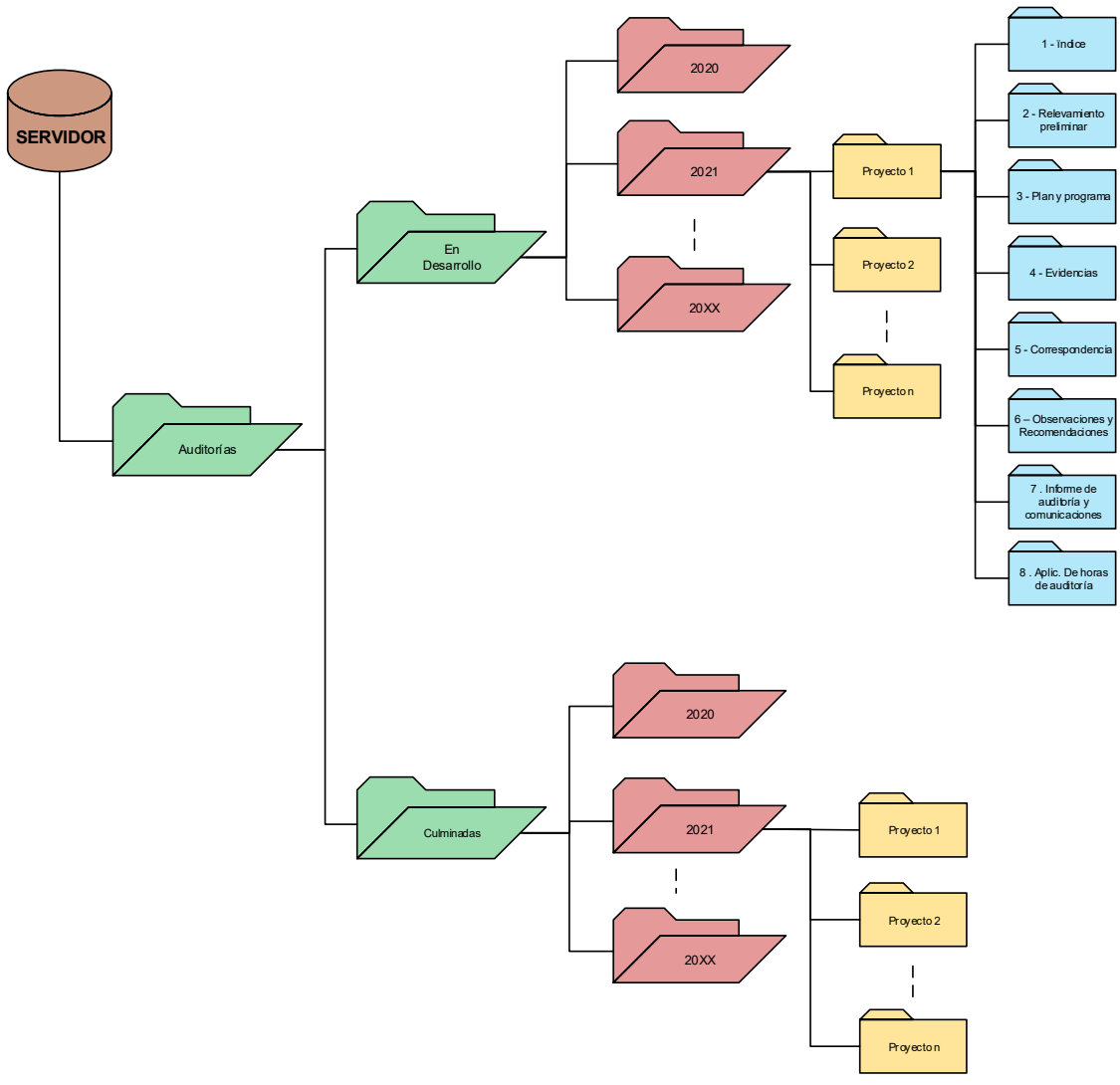
Como puede apreciarse en el gráfico precedente, el 36,4 % de las UAI que gestionan legajos digitales no posee ningún tipo de referenciación interna que permita relacionar la información dentro del propio legajo.

8. METODOLOGÍA PROPUESTA PARA LA ELABORACIÓN DE LEGAJOS DIGITALES

En el marco de los lineamientos contenidos en el **Anexo IV del Manual de Control Interno Gubernamental de la Sindicatura General de la Nación aprobado por Resolución SGN 3/2011**, referido a la administración de la documentación de auditoría, a continuación se describe la metodología propuesta para el tratamiento documental de los legajos digitales.

I. ORDENAMIENTO Y REFERENCIACIÓN

I.a. Para un adecuado ordenamiento y fácil acceso a la información a los proyectos de auditoría, se propone la siguiente estructura documental:



I.b. La información correspondiente a cada proyecto de auditoría en desarrollo deberá almacenarse en la carpeta del año que corresponda.

I.c. Los nombres de las carpetas que identifiquen a cada proyecto deberán contener el *Nro. de carga en el sistema SISAC* de acuerdo al plan de auditoría definido y aprobado, las siglas del *Organismo auditado,* la *Descripción del Proyecto y la clasificación de información* (ver punto III.a.), Ej.: 1.01 - RPI - GESTIÓN DE TI - R.

I.d. Cada legajo deberá contener, como mínimo, las subcarpetas que a continuación se detallan y que fueran expresadas gráficamente en el punto I.a, a fin de resguardar de manera ordenada la información correspondiente:

1 - Índice

Generar un archivo a través del cual pueda accederse al resto de las carpetas mediante hipervínculos.

2 - Relevamiento preliminar

Recopilar información de informes anteriores sobre el proceso a auditar, observaciones vigentes, normativa relacionada con el proyecto, identificación del ente auditado (domicilio, teléfonos, página web, autoridades, etc), información presupuestaria y de recursos humanos y manuales de procedimientos, entre otros.

3 - Plan y programa

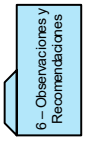
Almacenar información del proyecto definida en el Plan de auditoría (Objeto, procedimientos a realizar, plazos, recursos asignados, etc) y el programa de trabajo definido firmado digitalmente por los responsables del proyecto a través de la elaboración de un informe gráfico con firma conjunta (IFGRA) en el sistema GDE.

4 - Evidencias

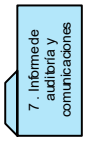
Reunir las evidencias resultantes de los procedimientos de auditoría aplicados. Las evidencias que den soporte a observaciones deberán firmarse digitalmente elaborando un informe gráfico (IF) a través del sistema GDE. Adicionalmente, una vez culminado el proyecto de auditoría deberá generarse un hash sobre la carpeta, a fin de garantizar su integridad.

5 - Correspondencia

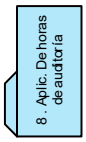
Llevar un registro de la correspondencia enviada al auditado y la recibida por parte de este en el marco del proyecto de auditoría ejecutado.



Detallar las observaciones formuladas resultantes de la auditoría realizada y vincularlas con las evidencias que las soportan a través de hipervínculos. Adicionalmente, deberá registrarse información respecto del curso de acción a seguir y la fecha de regularización prevista para cada observación, a fin de llevar a cabo el seguimiento respectivo.



Almacenar el informe de auditoría en sus versiones preliminares y final y las comunicaciones oficiales (CCOO) realizadas del mismo a través del sistema GDE. La versión final del informe deberá estar firmada digitalmente por los responsables de la ejecución del proyecto a través de la elaboración de un informe gráfico con firma conjunta (IFGRA) en el sistema GDE. Adicionalmente, deberá almacenarse la opinión del auditado respecto de los hallazgos detectados.



Especificar los recursos insumidos en la ejecución del proyecto de auditoría, detallando las horas de auditoría planificadas y ejecutadas por cada agente participante.

I.e. Una vez finalizado el proyecto de auditoría deberá trasladarse el legajo digital correspondiente a la carpeta "Culminados". Sobre dicha carpeta deberán aplicarse las medidas de seguridad necesarias que permitan garantizar la integridad del legajo, impidiendo el agregado, borrado o editado de la información allí contenida.

II. RESGUARDO DE LA INFORMACIÓN

II.a. La información deberá resguardarse y ser accesible por el tiempo establecido en "Las Normas de Auditoría Interna Gubernamental".

II.b. En el caso de que la Unidad de Auditoría Interna cuente con un repositorio de acceso compartido por todos los agentes para el resguardo de información digital, el resguardo de la información contenida en el Servidor de Archivos en el cual se alojan los datos es responsabilidad del área de sistemas del organismo, quien deberá implementar las medidas técnicas adecuadas a fin de garantizar su salvaguarda, a instancias de lo definido por la Unidad de Auditoría Interna.

II.c. En caso de no contar con dicho repositorio, la Unidad de Auditoría Interna deberá establecer un procedimiento propio para la salvaguarda de la información digital.

III. CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN

Las UAI poseen activos utilizados para el normal desarrollo de sus actividades y el cumplimiento de las funciones que le fueran asignadas por ley que deben ser protegidos adecuadamente de acuerdo a su sensibilidad y criticidad.

Todos los activos de información deben clasificarse de acuerdo a un criterio de clasificación pre-establecido, para luego proceder a su tratamiento, a fin de garantizar tanto su seguridad como su correcto uso, estableciendo niveles de protección proporcionales al riesgo.

III.a. Clasificación de la información

Puntualmente en el tema que nos ocupa, los legajos digitales deberán ser clasificados a fin de establecer los lineamientos básicos que permitan alcanzar y mantener una adecuada protección de la información contenida en ellos.

En tal sentido, el propietario de cada legajo digital será el supervisor responsable de la ejecución de cada proyecto, siendo el encargado de clasificarlo y de establecer los derechos de acceso en consenso con el Auditor Interno Titular.

El criterio de clasificación de la información adoptado en el que deberá basarse el supervisor responsable es el de “Confidencialidad” que se define como la característica que previene contra el acceso no autorizado a los activos de información, pudiendo clasificarse cada legajo de la siguiente manera:

1. **USO INTERNO (UI)**. Información que puede ser conocida y utilizada por todos los empleados de la UAI y algunas entidades externas debidamente autorizadas. Su divulgación o uso no autorizado podría ocasionar daños leves para la UAI, la Jurisdicción o terceros.

2. **RESTRINGIDA (R)**. Información que sólo puede ser conocida y utilizada por un grupo de empleados que la necesiten para realizar su trabajo. Su divulgación o uso no autorizado podría ocasionar daños significativos a la UAI, a la Jurisdicción o a terceros.

3. **CONFIDENCIAL (C)**. Información que sólo puede ser conocida y utilizada por el personal jerárquico y autorizado de la UAI. Su divulgación o uso no autorizado podría ocasionar daños graves a la UAI, a la Jurisdicción o a terceros.

III.b. Tratamiento de Información

Deberán aplicarse un conjunto de controles adecuados para el tratamiento de la información previamente clasificada, de acuerdo a un esquema predefinido.

En este sentido, para cada valor de clasificación otorgado a los legajos, deberán definirse los procedimientos de acceso, distribución, almacenamiento y destrucción, a saber:

INFORMACIÓN CONFIDENCIAL

- **Acceso**

El acceso al material clasificado como "Confidencial" será restringido al Auditor Interno Titular, Auditores Adjuntos, y al Supervisor responsable del proyecto y empleados que, en virtud de los requerimientos de su tarea o por los motivos que se determinen, hayan sido debidamente autorizados para ello, con los requisitos y limitaciones que en cada caso se establezcan.

Se deberán revisar y actualizar periódicamente los derechos de acceso a los recursos que contengan información confidencial.

- **Distribución**

La distribución de la información deberá estar basada en la "necesidad de conocer". Se deberán implementar controles a fin de garantizar que la distribución de la información se realice estrictamente al personal que necesite conocer dicha información para el desarrollo de sus tareas.

La distribución de material clasificado como "Confidencial" deberá estar aprobada por el auditor Interno Titular.

En caso de que sea necesaria la distribución de copias, se llevará a cabo con idénticas medidas de prevención que si del original se tratase.

- **Almacenamiento**

La información confidencial en formato digital deberá almacenarse cifrada y los medios, soportes e instalaciones de almacenamiento de información deberán poseer

adecuadas medidas de seguridad.

Queda prohibido el almacenamiento de información confidencial en estaciones de trabajo.

- **Destrucción**

El material clasificado como confidencial deberá ser destruido antes de ser desechado.

La destrucción del material clasificado como confidencial deberá ser aprobada por el Auditor Interno Titular y efectuada por personal autorizado.

El material deberá ser destruido de forma segura, a fin de evitar su reconstrucción o lectura posterior.

En cada proceso de destrucción deberá generarse un acta que identifique al personal actuante y la metodología empleada para la destrucción de la información. Dicha acta deberá ser firmada por el Auditor Interno Titular y el responsable del área de sistemas del organismo.

INFORMACIÓN RESTRINGIDA

- **Acceso**

El acceso a la información clasificada como "restringida" será limitado al Auditor Interno Titular, Auditores Adjuntos, y los Supervisores y empleados que, en virtud de los requerimientos de su tarea o por los motivos que se determinen, hayan sido debidamente autorizados para ello.

Se deberán revisar y actualizar periódicamente los derechos de acceso a los recursos que contengan información restringida.

- **Distribución**

La distribución de la información deberá estar basada en la "necesidad de conocer". Se deberán implementar controles a fin de garantizar que la distribución de la información se realice estrictamente al personal que necesite conocer dicha información para el desarrollo de sus tareas.

En caso de que sea necesaria la distribución de copias, se llevará a cabo con idénticas medidas de prevención que si del original se tratase.

- **Almacenamiento**

La información clasificada como restringida será almacenada bajo condiciones adecuadas para prevenir el acceso por parte de personas no autorizadas.

La documentación de uso restringido deberá guardarse cuando no esté siendo utilizada.

No deberá almacenarse información restringida en estaciones de trabajo.

Los medios y soportes que contengan información restringida deberán poseer adecuadas medidas de seguridad.

- **Destrucción**

El material clasificado como restringido deberá ser destruido antes de ser desechado.

La destrucción del material deberá ser efectuada por personal autorizado a través de medios que impidan la reconstrucción total o parcial de este.

En cada proceso de destrucción deberá generarse un acta que identifique al personal actuante y la metodología empleada para la destrucción de la información. Dicha acta deberá ser firmada por el Auditor Interno Titular y el responsable del área de sistemas del organismo.

INFORMACIÓN DE USO INTERNO

- **Acceso**

Sólo el personal que pertenezca a la Unidad de Auditoría Interna o externos debidamente autorizados a cumplir una tarea específica por un tiempo acotado, podrá tener acceso a la documentación de uso interno.

- **Distribución**

La distribución de la información deberá estar basada en la "necesidad de conocer". Se deberán implementar controles a fin de garantizar que la distribución de la información se realice al personal que necesite conocer dicha información para el desarrollo de sus tareas.

- **Almacenamiento**

La información clasificada como de uso interno será almacenada bajo condiciones adecuadas para prevenir el acceso por parte de personas no autorizadas.

La documentación de uso interno deberá guardarse cuando no esté siendo utilizada.

No deberá almacenarse información de uso interno en estaciones de trabajo.

- **Destrucción**

El material clasificado como de uso interno deberá ser destruido antes de ser desechado. La destrucción del material deberá ser efectuada por personal autorizado a través de medios que impidan su reconstrucción total o parcial de este.

9. CONCLUSIONES

Teniendo en cuenta que la despapelización en el Sector Público Nacional es uno de los principios básicos en los que se sustenta la idea de Gobierno Electrónico, con la finalidad de alcanzar la simplificación de los trámites de la gestión administrativa, la estandarización de los procesos y al aumento de la eficacia y eficiencia de la gestión, y considerando que la Administración Pública en general no puede permanecer ajena a los avances tecnológicos y al empleo de los nuevos medios que el desarrollo innovativo provee, orienté el desarrollo del trabajo integrador final de la Especialización en Auditoría Interna Gubernamental a la presentación de una iniciativa innovadora para el fortalecimiento del sistema de control interno, a partir de la incorporación de la tecnología en la gestión documental en las Unidades de Auditoría Interna.

Para ello, llevé a cabo un relevamiento del contexto actual en el que se encuentran las Unidades de Auditoría Interna, respecto de la metodología utilizada para la gestión de la documentación que sustenta los respectivos proyectos de auditoría ejecutados. El análisis de dicha labor arrojó que un alto porcentaje de las UAI encuestadas aún utilizan legajos físicos como soporte documental de sus proyectos de auditoría, vislumbrando en otros casos una incipiente utilización de herramientas tecnológicas para la gestión documental, aunque sin definiciones metodológicas claras y homogéneas respecto de algunas cuestiones como ser, la estructura de los legajos, el sistema de referenciación, las medidas que garanticen la inviolabilidad de la información contenida en los legajos, entre otras.

Por lo expuesto, entiendo que resulta necesario reformular el sistema de gestión y administración de la documentación de auditoría, a fin de incorporar las ventajas que ofrecen las Nuevas Tecnologías de la Información y Comunicación.

En tal sentido, en el punto 8 del presente, propongo una metodología alternativa para sustituir las técnicas tradicionales de gestión de la documentación, incorporando la

utilización de la tecnología para la administración de los documentos a partir de la conformación de legajos digitales de auditoría, estableciendo un adecuado sistema de ordenamiento y referenciación de la documentación contenida en dichos legajos, planteando y describiendo la necesidad de implementar medidas respecto del resguardo, clasificación y tratamiento de la información, a fin de garantizar la confidencialidad, disponibilidad e integridad de la información.

Por último, cabe comentar que la implementación de la metodología propuesta por parte de las Unidades de Auditoría Interna como soporte sustituto del papel, redundaría en beneficios múltiples, tales como aumento de la eficiencia en el tratamiento de los procesos, ahorro de recursos naturales y preservación del medio ambiente, mayor confidencialidad de la información contenida en los documentos, optimización de espacios físicos, reducción de los costos de almacenamiento y de traslado de documentación y perdurabilidad de la información.

10. GLOSARIO

Firma digital: La ley 25.506 define a la firma digital como el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose esta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Firma electrónica: La ley 25.506 define a la firma electrónica como el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

Documentación de auditoría: Documentación que respalda la tarea efectuada para la emisión de un informe, sea este de auditoría, de control, evaluación o de otro tipo.

Documentos particulares no firmados: Archivos de trabajo en cualquier de los formatos electrónicos (pdf, Word, Excel, correos electrónicos, bases de datos, etc.).

Documentos digitales: Archivos de trabajo en cualquiera de los formatos electrónicos, sobre los cuales el responsable firmante ha procedido a incorporar su firma digital.

11.BIBLIOGRAFÍA CONSULTADA

Ley 24156. (1992). *Administración financiera y de los Sistemas de Control del Sector Público Nacional*. Buenos Aires, Argentina: Boletín oficial de la RA: 26/08/1992 Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/554/texact.htm.

Ley 25506. (2001). *Firma Digital*. Buenos Aires, Argentina: Boletín oficial de la RA: 11/12/2001 Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

Decreto Nº *378*. (2005). Poder Ejecutivo Nacional. *Plan Nacional de Gobierno Electrónico y planes sectoriales. Lineamientos estratégicos.* Buenos Aires, Argentina: Boletín oficial de la RA: 27/04/2005 Disponible en http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=105829

Decisión Administrativa Nº *669*. (2004). Jefatura de Gabinete de Ministros. *Política de Seguridad de la Información.* Buenos Aires, Argentina: Boletín oficial de la RA: 20/12/2004 Disponible en http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=102188

Resolución Nº *48*. (2005). Sindicatura General de la Nación. *Norma de Control Interno para Tecnología de la Información* .Buenos Aires, Argentina: Boletín oficial de la RA: 05/05/2005 Disponible en http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=106452

Resolución Nº 152. (2002). Sindicatura General de la Nación. *Normas de Auditoria Gubernamental.* Buenos Aires, Argentina: Boletín oficial de la RA: 17/10/2002 Disponible en http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=79051

12.ANEXO

Encuesta sobre la gestión documental en las Unidades de Auditoría Interna

1. En la Unidad de Auditoría Interna donde se desempeña los documentos resultantes de la ejecución de los proyectos y actividades de auditoría se resguardan en:

   ◯ a) Legajos físicos

   ◯ b) Legajos digitales

   ◯ b) Legajos mixtos

2. Si en el transcurso de una auditoría le remiten información digital como evidencia de algún procedimiento, que hacen con dicha evidencia?:

   Seleccione todas las opciones que correspondan.

   ☐ a) Se imprime para conformar el legajo físico de auditoría.

   ☐ b) Se guarda el archivo digital en la PC del Supervisor o Auditor Responsable del proyecto o actividad en una carpeta creada al efecto.

   ☐ c) Se guarda el archivo digital en un repositorio compartido para la conformación del legajo digital.

   ☐ d) Es firmada digitalmente por el Supervisor/Adjunto o Auditor Responsable del proyecto o actividad.

   ☐ Otros: _____

3. Posee la Unidad de Auditoría Interna un procedimiento para la elaboración de legajos digitales que defina, entre otras cuestiones, una estructura uniforme para su conformación?

   ◯ Sí

   ◯ No

4. Posee la Unidad de Auditoría Interna un repositorio de acceso compartido por todos los agentes para el resguardo de información digital?

- ◯ Sí
- ◯ No

5. Se lleva a cabo algún procedimiento para garantizar la inalterabilidad de los legajos digitales una vez culminada la auditoría?

- ◯ Sí
- ◯ No

6. Se llevan a cabo copias de resguardo de los legajos digitales? *

Selecciona todas las opciones que correspondan.

- ☐ Sí
  - ☐ a) Las copias de respaldo las realiza la propia UAI.
  - ☐ b) Los backups los realiza el área de sistemas a pedido de la UAI.
  - ☐ c) Hay un procedimiento definido de backups que se ejecuta automáticamente del cual el área de sistemas es el responsable.
  - ☐ d) d) Otro:
- ☐ No

7. Poseen los legajos digitales algún mecanismo de referenciación interna que relacione, por ejemplo, las evidencias con los hallazgos detectados?

- ◯ Sí
- ◯ No