Universidad Siglo 21

Proyecto Trabajo Final de Graduación

Licenciatura en Informática

Proyecto de Aplicación Profesional (PAP)

Manual de Normas y Procedimientos de Auditoría Informática Auditoría General de la Nación

Resumen

El presente trabajo tiene como objetivo cubrir la necesidad que se observó en la Auditoría General de la Nación (AGN) de disponer de un Manual de Normas y Procedimientos de Control Externo Gubernamental de Tecnologías de la Información.

La etapa de proyecto describe la necesidad detectada, muestra un relevamiento del ciclo de vida de una auditoría informática, y refiere en forma sintética las principales normas internacionales a las que se ajusta el trabajo como por ejemplo COBIT, ISO 27000, ITIL, CMMI entre las más importantes.

El Manual está alineado con la normativa existente en la AGN, principalmente con las Normas de Control Externo Gubernamental aprobadas por el organismo. Los procedimientos enunciados en el manual cubren todos los aspectos que deben ser evaluados en una auditoría de Tecnologías de la Información y Comunicaciones (TIC), como por ejemplo organización del área de TIC, desarrollo de aplicaciones, infraestructura de TIC, seguridad de la información, entre otros.

Si bien este manual fue desarrollado para la AGN, puede ser fácilmente adaptado para ser utilizado por otras organizaciones tanto públicas como privadas.

Se busca que este documento permita al Departamento de Auditoría Informática de la AGN realizar trabajos estandarizados, con criterios claros y precisos. De esta forma se obtendrán informes de auditoría de alta calidad que permitan lograr un mejor uso de las TIC en el ámbito del Sector Público Nacional.

Palabras Clave: Auditoría Informática, Auditoría General de la Nación, Manual de Normas y Procedimientos, Control Externo Gubernamental.

Abstract

The goal of this work is to cover the need observed at the National Audit Office of the Argentinean Nation (Auditoría General de la Nación - AGN) to have a Manual of Standards and Procedures for Government External Control of Information Technology.

The project stage describes the detected need, shows a lifecycle survey of an Information and Communications Technologies (ICT) audit, and briefly refers to the main international standards to which the is adjusted, such as COBIT, ISO 27000, ITIL, CMMI, among the most important.

The Manual is aligned with the existing regulations at the AGN, mainly with the Government's External Control Standards approved by the agency. The procedures stated in the manual cover all the topics that should be evaluated in a ICT audit, such as ITC Area Organization, Application Development, ITC Infrastructure, ITC Security, among others.

Although this manual was developed for AGN, it could be easily adapted to be used by other organizations, both public and private.

It is sought that this document allows the ITC Audit Department from the AGN to perform standardized work, with clear and precise criteria. Consequently, high-quality audit reports will be obtained to achieve better use of ITC in the area of the National Government Agencies.

Key words: Information Audit, Auditoría General de la Nación, Manual of Standards and Procedures, Government External Control.

Tabla de contenido

Tabla de imágenes:

1. Título

Desarrollo de un manual de normas y procedimientos para la ejecución de auditorías de Tecnologías de la Información y Comunicaciones en el ámbito de la Auditoría General de la Nación.

2. Introducción - Marco de referencia institucional

2.1 Antecedentes

La Auditoría General de la Nación (AGN) es un organismo creado por la Ley 24.156, Ley de Administración Financiera y de los Sistemas de Control del Sector Público Nacional, sancionada el 30 de setiembre de 1992 (Honorable Congreso de la República Argentina, 1992). Estos últimos comprenden a las estructuras de control interno y externo del Sector Público Nacional (SPN), siendo la Sindicatura General de la Nación (SIGEN) y la Auditoría General de la Nación respectivamente, los órganos rectores de estos sistemas de control.

La AGN se crea como un ente de control externo del SPN dependiente del Congreso Nacional y se le confiere independencia funcional, lo que le permite dictar sus propias normas internas. Tiene como funciones realizar auditorías de gestión, exámenes especiales, evaluaciones de programas, proyectos y operaciones en los organismos y entidades que estén bajo su control. La ley establece que deberá formular los criterios de control y auditoría estableciendo las normas necesarias para la realización de sus tareas.

La AGN adquiere rango constitucional a partir de la Reforma Constitucional del año 1994 (Asamblea Constituyente, 1994) que en el Capítulo Sexto – De la Auditoría General de la Nación, artículo 85 la define como *"...organismo de asistencia técnica del Congreso…",* que *"… Tendrá a su cargo el control de legalidad, gestión y auditoría de toda la actividad de la administración pública centralizada y descentralizada, cualquiera fuera su modalidad de organización…".*

De acuerdo a esto último la AGN está encargada de controlar la gestión, es decir aquellos actos en los cuales el orden jurídico establece de antemano qué es específicamente lo que los funcionarios públicos deben cumplir en el ejercicio de sus funciones, sin emitir opinión sobre actos realizados de acuerdo a sus facultades discrecionales (Natale, 1995).

2.2 Descripción del área problemática

En 2001, la AGN crea mediante la Resolución N° 244/01 - AGN (Auditoría General de la Nación, 2001) el Departamento de Auditoría Informática y Sistemas. Dentro de su responsabilidad primaria se encuentran las tareas de programar, coordinar, supervisar y ejecutar las acciones necesarias para evaluar en el SPN la consistencia, compatibilidad, integridad y seguridad de los sistemas informáticos, como así también, la calidad, actualidad y legalidad de la tecnología de información utilizada. Dado que el organismo no dictó una norma específica para la ejecución de las tareas asignadas, se eligió como modelo de trabajo a COBIT 2 (Control OBjectives for Information and Related Technology). En base a éste, se creó una serie de cuestionarios y listas de verificación que establecieran un mínimo estándar de trabajo. Posteriormente se evolucionó a la versión 3 y se desarrolló una herramienta informática, programada mediante ORACLE Forms, utilizando un motor de base de datos ORACLE que automatizaba parte de la redacción del informe de auditoría y la asignación de los índices de madurez a cada uno de los puntos de control de COBIT.

Hasta el año 2004, además de las tareas propias de auditoría, el Departamento de Auditoría Informática y Sistemas se ocupaba del desarrollo, análisis, diseño, implementación y mantenimiento de toda la infraestructura informática de la AGN. Esto generaba inconvenientes en la gestión tanto de las tareas de auditoría como aquellas inherentes a un área de sistemas. Para solucionar este problema, la AGN a través de la Resolución N° 67/04 - AGN (Auditoría General de la Nación, 2004) separa las funciones de Auditoría Informática y la de Sistemas.

Con la publicación de la version 4 de COBIT se comienza a trabajar con este estándar utilizándolo como plantilla de trabajo hasta el año 2016, donde producto de un proceso de reingeniería de todo el organismo este modelo sólo queda como referencia de buenas prácticas.

En el año 2015 la AGN publica un documento denominando “Normas de Control Externo Gubernamental” (Auditoría General de la Nación, 2015) en la cual se establecen las políticas de alto nivel que deben regir las tareas de auditoría externa para el SPN. Además, se comienza con la implementación de un software denominado SICA (Sistema Integrado de Control de Auditorías), que se utilizará para el registro y control de todas las tareas asociadas a la ejecución de una auditoría.

Para la implementación de este sistema, cada una de las áreas debe definir un conjunto de procesos y procedimientos específicos que quedarán registrados en el sistema cuando se ejecuten las distintas auditorías.

La necesidad de sistematizar todas las tareas de control que realiza el Departamento de Auditoría Informática brinda la oportunidad de completar este trabajo con la redacción de un Manual de Normas y Procedimientos que dé el soporte formal necesario.

Los cambios producidos en el organismo generan la necesidad de desarrollar un manual de procedimientos de auditoría informática que abandone el paradigma anterior, en el cual se realizaban exclusivamente auditorías informáticas, para pasar a uno más abarcativo que incluya todo el espectro de las Tecnologías de la Información y Comunicaciones (TIC). El avance en el uso de las nuevas tecnologías en todo el ámbito del estado nacional hace necesario que el Departamento de Auditoría Informática tenga procedimientos definidos y uniformes para la realización de los trabajos asignados, y los mismos estén adecuados a las nuevas tecnologías.

2.3 Formulación de la problemática

¿Cómo establecer un proceso formal de auditorías de TIC dentro del ámbito del Departamento de Auditoría Informática de la Auditoría General de la Nación que sintetice las distintas normas existentes en la actualidad?

2.4 Justificación

El Departamento Auditoría Informática no cuenta en la actualidad con un manual de normas formalmente aprobado para la realización de los trabajos de auditoría que debe realizar, ni cuenta con un manual de procedimientos que detallen cómo deben ejecutarse dichas tareas. Hasta la fecha, se trabajó básicamente con metodologías *ad hoc*, definidas en cada caso por el equipo de auditoría actuante y aprobadas informalmente por el jefe de ese departamento.

Toda la situación descripta tuvo como consecuencia la falta de estandarización en los productos que el departamento producía ya que el enfoque de los mismos dependía de la visión personal de los miembros del equipo de auditoría.

En 2016 existe una tentativa de corrección de esta situación con la aprobación por parte del Colegio de Auditores Generales de la Nación de las “Normas de Control Externo

de la Gestión Gubernamental" (Auditoría General de la Nación, 2016) que incluye a las auditorías informáticas como un tipo particular de auditoría de gestión. El problema que presenta la aplicación estricta de esta normativa es la falta de un enfoque técnico preciso para las tareas de auditorías informáticas. Esta norma pone énfasis en los conceptos de economía, eficiencia, eficacia y equidad, pero omite toda referencia a los de integridad, confidencialidad y disponibilidad que son centrales en las auditorías informáticas.

La otra deficiencia que presenta la falta de una norma específica es que no considera el cambio de paradigma que se produce debido a la convergencia entre las tecnologías que dan soporte a los sistemas de información y las comunicaciones.

Los motivos enunciados justifican la redacción de un Manual de Normas y Procedimientos de Control Externo de Tecnologías de la Información y Comunicaciones.

La redacción, aprobación y puesta en uso de este manual representará para la AGN una mejora sustancial en los procesos de auditaría, no solamente para las específicas del área en cuestión sino también como apoyo a auditorías financieras o contables que necesiten auditorías en los sistemas de información para asegurar que los datos que se extraen de los mismos sean confiables.

El principal problema que se presenta en la redacción de estas normas es que actualmente existen variados estándares de la industria para el control de la gestión de TIC. Por este motivo, la idea de este desarrollo es generar un manual de procedimientos que integre estas normativas generando un único protocolo de controles y pruebas.

Dentro de los más utilizados podemos mencionar a COBIT en sus versiones 4 y 5, ITIL (Information Technology Infrastructure Library - Biblioteca de Infraestructura de Tecnologías de Información), PMBOK (Project Management Body of Knowledge - Fundamentos para la Dirección de Proyectos), normas ISO (International Organization for Standardization – Organización Internacional de Estandarización), normas TIER (del Uptime Institute), BSI (British Standards Institution – Instituto Británico de Estandarización) , y técnicas de auditorías como las basadas en riesgos, Auditoría de Valor (Audit For Value), entre otras.

Muchas de las normas mencionadas y otras vinculadas a esta temática se superponen entre sí, o constituyen enfoques distintos de la misma problemática. Esto podría llevar a que diferentes equipos de trabajo del Departamento de Auditoría Informática, que realizan tareas similares en los organismos del SPN, utilicen parámetros

disímiles en sus análisis. Esto tiene como consecuencia para el Departamento de Auditoría Informática la falta de consistencia en sus informes.

Este trabajo permitirá a la AGN disponer de un enfoque único en la realización de sus informes de auditoría de TIC. La aplicación de procedimientos formalmente definidos en todos los trabajos de control permitirá la redacción de informes con una única visión mejorando la calidad general del trabajo del Departamento de Auditoría Informática.

Los informes de la AGN están dirigidos en primera instancia al Congreso Nacional, pero además, por estar los mismos publicados en Internet para que toda la sociedad pueda consultarlos, también tiene como destinatario toda la ciudadanía.

Este trabajo busca presentar una metodología que abarque las normativas existentes en materia de controles de gestión de TIC, muchas de las cuales se superponen en algunos aspectos, o se enfocan desde distintas visiones. Se trata de tomar esta base y desarrollar una plataforma única de trabajo.

3. Objetivos

3.1 Objetivo general del proyecto

Desarrollar un Manual de Normas y Procedimientos para Auditoría Informática que contemple la normativa existente para el control externo gubernamental de los organismos del Sector Público Nacional.

3.2 Objetivos específicos del proyecto

- Entender las disposiciones legales que regulan las auditorías externas que se realizan al SPN.
- Entender la posición del Departamento de Auditoría Informática dentro de la estructura de la AGN.
- Entender la estructura interna del Departamento de Auditoría Informática.
- Determinar la normativa existente en materia de auditoría y controles de TIC que son aplicables para cumplir con el objetivo buscado.
- Formular procedimientos que sinteticen la normativa relevada.

4. Límite

El manual debe definir todos los procedimientos que debe realizar un equipo de auditoría desde que se le asigna el proyecto hasta que el informe está terminado. Debe cubrir todos los posibles análisis que se puedan solicitar al Departamento de Auditoría Informática.

Los principales elementos posibles de auditar son:

- Aspectos legales y normativos.
- Administración de proyectos de TIC.
- Desarrollo de aplicaciones.
- Procesos y operaciones de TIC.
- Seguridad física y lógica.
- Infraestructura tecnológica.
- Comunicaciones y redes.
- Aplicaciones WEB.
- Aplicaciones móviles.
- Bases de datos.
- Soporte a usuarios.

5. Alcance

El trabajo se centra en los procesos de auditoría comprendidos en las siguientes etapas:

- Planificación de la auditoría
- Ejecución
- Conclusión y redacción del informe.

6. No Contempla

Este proyecto no contempla el desarrollo de un sistema informático que de soporte a los relevamientos indicados en el manual de procedimientos.

7. Marco Teórico

7.1 Actividad del cliente

La AGN es un organismo técnico que depende del Congreso Nacional, a quien asesora realizando las tareas de control externo gubernamental.

De acuerdo a la Ley N° 24.156 (Honorable Congreso de la República Argentina, 1992), la máxima autoridad del organismo es el Colegio de Auditores Generales formado por un Presidente elegido por el partido de la oposición con mayor representación parlamentaria, y por seis Auditores Generales, elegidos tres por la Cámara de Senadores y tres por la Cámara de Diputados respetando la proporción de mayorías y minorías de cada cámara.

La misión, visión y valores del organismo se encuentran en su página web (Auditoría General de la Nación, 2017) y son:

> *"**Misión***
>
> *Somos un organismo constitucional con autonomía funcional que asiste técnicamente al Congreso de la Nación en el ejercicio del control externo del Sector Público Nacional mediante la realización de auditorías y estudios especiales para promover el uso eficiente, económico y eficaz de los recursos públicos y contribuir a la rendición de cuentas y sus resultados para el perfeccionamiento del Estado en beneficio de la sociedad.*
>
> ***Visión***
>
> *Ser un organismo de excelencia en el control que contribuya a mejorar la gestión pública en beneficio de la sociedad.*
>
> ***Nuestros valores***
>
> ***Independencia:** con respecto a la entidad fiscalizada y otros grupos de intereses externos.*
> ***Objetividad:** en el tratamiento de las cuestiones o los temas sometidos a revisión.*
> ***Compromiso Institucional:** en el cumplimiento de nuestras funciones.*

> ***Probidad:*** *observando una conducta y un desempeño honesto y leal de la función o cargo, con preeminencia del interés general sobre el particular.*
> ***Profesionalismo:*** *en la realización del trabajo con el objeto de desempeñar nuestras responsabilidades de manera competente y con imparcialidad.*
> ***Ética:*** *en relación al conjunto de valores y principios que guían la labor cotidiana."*

La AGN realiza distintos tipos de auditorías según las temáticas que abarquen las mismas. Éstas pueden ser financieras, entre ellas la aprobación de la Cuenta de Inversión de la República Argentina o de los estados contables de los distintos organismos que componen el SPN, o de control de gestión en general. Dentro de estas últimas, por su importancia estratégica, merecen especial consideración las de control ambiental y las informáticas.

Las auditorías informáticas o de TIC son realizadas por el Departamento de Auditoría Informática. Éste fue creado en el año 2001 y dentro de sus actuales misiones y funciones, establecidas por la Resolución N° 67/04 - AGN (Auditoría General de la Nación, 2004), se encuentran:

- *"Ejecutar la auditoría de los sistemas centrales de información operables en el órgano de coordinación de la Administración Financiera".*
- *"Ejecutar relevamientos en los organismos del Sector Público Nacional competentes en los aspectos de definición de política informática de la Administración Pública Nacional en cuanto al ejercicio de tales funciones".*

Este departamento depende estructuralmente de la Gerencia de Planificación y Proyectos Especiales, que es en primera instancia quien lo controla.

7.2 Conceptos generales sobre auditorías

7.2.1 En qué consiste una auditoría

De acuerdo con la Real Academia Española el término (Real Academia Española, 2017) se define como:

1. f. Revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse.

2. f. Revisión y verificación de las cuentas y de la situación económica de una empresa o entidad.

3. f. Empleo de auditor.

4. f. Tribunal o despacho del auditor.

Para este trabajo, la acepción más importante es la primera. En ella se expresan conceptos fundamentales, primero es "sistemático", es decir no es una actividad que se realiza en forma aleatoria o sin un plan definido, por el contrario, una auditoría es una tarea pautada dentro de un proceso, que se realiza en momentos determinados de antemano, y consta de una serie de procesos y técnicas formalmente definidas para obtener los resultados buscados.

Existen distintas clasificaciones y tipos de auditorías, principalmente se pueden agrupar de acuerdo a quienes las realizan o de acuerdo a su objeto.

En el primer caso se pueden dividir en:

- Auditorías Internas: de acuerdo a la definición proporcionada por el Instituto de Auditores Internos de Argentina "...es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno…" (Instituto de Auditores Internos de Argentina, 2017). Su principal característica es que el equipo de auditoría actuante es personal propio de la empresa. Organizacionalmente en general, el área de Auditoría Interna es independiente de todas las gerencias, y reporta directamente al directorio o la máxima autoridad jerárquica del ente.
- Auditorías Externas: es un proceso de evaluación sistemático, exhaustivo, crítico y detallado de un determinado sistema de una empresa, como por ejemplo el sistema contable, la capacidad de financiación, el departamento de recursos humanos, su sistema informático, o cualquier otro aspecto vinculado a la gestión del organismo. Una auditoría externa puede ser obligatoria o voluntaria. A diferencia de las auditorías internas, el estudio se realiza por personal ajeno a la empresa, el objetivo es obtener una opinión independiente que dé credibilidad frente a terceros, ya que muchas veces estos análisis se realizan a solicitud de organismos regulatorios o entidades crediticias. Esto se realiza para determinar la razonabilidad, integridad y autenticidad de los estados analizados, y poder conocer la situación de sus activos y pasivos. El

procedimiento de auditoría externa será realizado por una persona o entidad especializada ajena a entidad, capaz de brindar una opinión independiente y de emitir al final del proceso un informe completo sobre el estado del sistema analizado.

Si en cambio se las agrupa por su objetivo, se pueden clasificar en:

- Auditorías Financieras: evalúa si los estados financieros de un ente están expresados según las normas legales y profesionales vigentes, y si reflejan efectivamente el estado financiero del auditado.
- Auditorías Contables: se realizan para evaluar si los procedimientos realizados por el contador están ajustados a las normas profesionales.
- Auditorías Médicas: es un proceso para, por un lado, evaluar la necesidad de la realización de un determinado tratamiento médico y, por otro, analizar el resultado de un tratamiento médico con el objetivo de mejorar el mismo.
- Auditorías de Gestión:. consiste en un examen independiente, objetivo y fiable de si las iniciativas, sistemas, operaciones, programas, actividades u organizaciones funcionan con arreglo a los principios de economía, eficiencia y eficacia, y si existe margen de mejora (Tribunal de Cuentas Europeo, 2017).
- Auditorías Informáticas: el INTOSAI (International Organisation of Supreme Audit Institutions - Organización Internacional de las Entidades Fiscalizadoras Superiores) define como Auditoría de TI al proceso que garantiza que el desarrollo, la implementación y el mantenimiento de los sistemas de TI cumplen con los objetivos del negocio, protegen el valor de la información y mantienen la integridad de los daros (International Organisation of Supreme Audit Institutions, 2013).

La Auditoría General de la Nación distingue tres tipos de auditorías (Auditoría General de la Nación, 2015):

- "*Auditoría Financiera: destinada a determinar si la información financiera de una entidad se presenta de conformidad con el marco de referencia y regulatorio aplicable. Busca reunir evidencia válida y suficiente para poder emitir una opinión sobre si la información financiera reflejada en los estados financieros bajo análisis carece de errores o fraudes que alteren significativamente esa información.*
- *Auditoría de Gestión: busca determinar si los proyectos, programas y/o entidades se desempeñan de conformidad con los principios de economía, eficiencia, eficacia y efectividad y si existen aspectos que puedan ser mejorados. La gestión deberá examinarse contra el marco de criterios adecuados, los desvíos en relación a esos*

criterios determinarán los hallazgos. El trabajo de auditoría incluirá el análisis de las causas que originan las desviaciones respecto de estos criterios. Las tareas deben tener como objetivo concluir sobre las cuestiones críticas auditadas y la posibilidad de introducir mejoras en las cuestiones revisadas.

- *Auditorías de Cumplimiento: busca determinar si una materia en particular cumple con las normas y regulaciones identificadas como criterios aplicables. En este sentido evalúa si las actividades, transacciones financieras y la información se desarrollaron ajustándose al marco regulatorio vigente en la entidad auditada. Estas regulaciones incluyen códigos, leyes, decretos reglamentarios, resoluciones, disposiciones presupuestarias, políticas establecidas, contratos firmados o principios generales de buena administración de recursos públicos."*

Además de estos tres tipos principales de auditorías, dentro de las Auditorías de Gestión se menciona un grupo más llamado auditorías especializadas, que requieren un enfoque técnico especifico. Entre ellas se encuentran las relacionadas con el Medio Ambiente, Deuda Pública, Sostenibilidad, Tecnologías de la Información y Comunicaciones, entre otras.

7.2.2 Ventajas en el uso de auditorías

Como ya se mencionó en puntos anteriores existen muchas variadas razones que justifican la realización de auditorías en las organizaciones ya sean del ámbito privado o del sector público.

La principal ventaja de la realización de auditorías es que permiten obtener información certera sobre distintos aspectos de la gestión de la empresa.

Es importante que el organismo auditado y el área bajo estudio consideren a la auditoría no como un examen con una visión negativa sobre las tareas que se realizan, sino como una oportunidad de mejora que permitirá a la organización cumplir sus objetivos con mayor eficiencia, economía y eficacia.

Las organizaciones deben diseñar un plan de auditorías que permita a la misma un exhaustivo control sobre los aspectos relevantes de su operación y gestión y con los resultados de las mismas implementar un plan de mejora continua.

Es importante que se establezca entre el auditado y el equipo de auditoría un ambiente de colaboración donde ambas partes contribuyan a obtener el mejor resultado

posible en beneficio de la organización. Debe quedar claro que una auditoría es un trabajo en equipo entre ambas partes y no una competencia entre las mismas.

7.2.3 Campos en los cuales se aplica

Los procesos de auditoría pueden aplicarse a todos los procesos de una organización y todos sus sectores dependiendo del objeto de la misma.

En el tema específico que cubre este trabajo, que son las auditorías de TIC, las áreas involucradas son prácticamente toda la empresa.

En la actualidad, el rápido avance de la tecnología en materia de procesamiento de datos, la disminución de costos en el equipamiento, y la convergencia entre la informática y las comunicaciones transformó al área de TIC en un área transversal a toda la organización. De esta forma brinda servicios a todos los sectores de la misma. Por este motivo, una auditoría de TIC debe forzosamente tener en cuenta este concepto y abarcar prácticamente toda la empresa.

Esta evaluación global implica analizar las acciones de dirección de la empresa, en particular de las gerencias de primer nivel que son las encargadas de impulsar los proyectos informáticos que serán utilizados por toda la organización, por lo que deberán ser verificadas las políticas organizacionales y su vínculo con las políticas TIC.

Como es obvio en este tipo de auditorías, las áreas de sistemas y de comunicaciones deben ser analizadas en forma exhaustiva, controlando todo el ciclo de vida de desarrollo de un sistema, desde la captura del/de los requerimiento/s hasta la puesta en producción y soporte del mismo. Deben examinarse en forma cuidadosa las políticas y procedimientos de seguridad informática, haciendo foco en el mantenimiento de la integridad, confidencialidad y disponibilidad de la información y en el correcto cuidado de todos los activos informáticos del ente bajo estudio. Para ello deben verificarse desde las políticas de uso de los bienes informáticos hasta la revisión de la gestión de usuarios, de la implementación de los firewalls, de zonas desmilitarizadas (DMZ - demilitarized zone), las configuraciones de los antivirus, software de detección de intrusos y cualquier otro aspecto vinculado a la seguridad de la información. Además, debe ser analizado el estado de la infraestructura que debe soportar todo el hardware y software del organismo, incluyendo el centro de datos, sistemas de energía, sistemas de control ambiental, sistemas de control de acceso, de detección y extinción de incendios, entre otros.

También deben ser tenidas en cuenta las áreas usuarias de los sistemas, para poder determinar si las mismas cumplen con lo que éstas necesitan para realizar sus tareas en forma eficaz y eficiente. Lo mismo que deberán ser analizadas las áreas de RR.HH. para determinar si existen y se cumplen políticas de ingreso de personal y fundamentalmente la existencia de planes de capacitación para el uso de los sistemas tanto por parte de los usuarios como del personal del área de sistemas para mantener sus capacidades técnicas actualizadas.

Como puede observarse las auditorías de TIC involucran a toda una organización.

7.3 TIC (Tecnologías de la Información y Comunicaciones)

7.3.1 COBIT 4

COBIT (*Control OBjectives for Information and Related Technology* - Objetivos de Control para Información y Tecnologías Relacionadas) es una guía de buenas prácticas. Es mantenida por ISACA (*Information Systems Audit and Control Association*) y por IT GI (*IT Governance Institute*). Esta versión se publicó en diciembre de 2005 y tuvo una mejora (COBIT 4.1) publicada en mayo del 2007 (IT Governance Institute, 2007).

COBIT propone que el aseguramiento del valor de TIC, la administración de los riesgos asociados y el aumento de los requerimientos para el control de la información son elementos clave en el gobierno de cualquier organización.

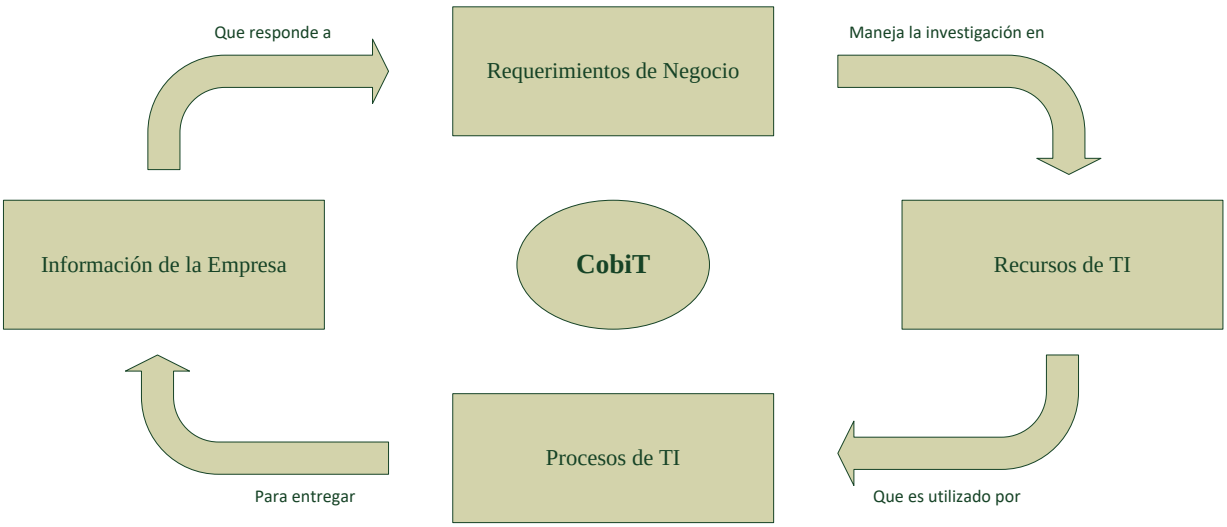
Básicamente COBIT es un marco de trabajo que permite a la empresa asegurar que:

- TI esté alineada con el negocio.
- TI ayude a maximizar los beneficios.
- El uso de los recursos de TI sea responsable.
- Los riesgos de TI se administren apropiadamente.

COBIT es una familia de productos formado por distintas guías y manuales, entre los cuales podemos mencionar el Resumen Informativo al Consejo sobre el gobierno de TIC, la Guía de Implementación de Gobierno de TI usando COBIT y Val IT, la Guía de Aseguramiento de TI usando COBIT, entre otros.

Es posible representar el marco de trabajo de COBIT mediante el siguiente esquema:

Ilustración 1 - Marco de Trabajo de COBIT 4



Fuente: Elaboración propia.

COBIT pone énfasis en que los objetivos de TI deben estar alineados y soportar los objetivos de la organización. Para ello, brinda un marco de buenas prácticas por medio de objetivos de control definidos agrupados por dominios, que están enfocados en el control de los procesos.

Se definen siete criterios que debe poseer la información:

- Efectividad.
- Eficiencia.
- Confidencialidad.
- Integridad.
- Disponibilidad.
- Cumplimiento.
- Confiabilidad.

COBIT clasifica los recursos en aplicaciones, infraestructura y personas, y sobre los mismos se aplican los objetivos de control.

Para la evaluación de cada uno de los objetivos de control COBIT da una serie de métricas y modelos de madurez, e identifica las responsabilidades asociadas a cada proceso de TI.

El modelo COBIT en su versión 4 se divide en 34 objetivos de control agrupados en 4 dominios tal como se describen en la siguiente tabla:

Tabla 1 - Modelo COBIT 4

Dominio 1 Planificar y organizar (PO)	PO1 – Definir un plan estratégico de TI
	PO2 – Definir la arquitectura de la información
	PO3 – Determinar la dirección tecnológica
	PO4 – Definir los procesos, organización y relaciones de TI
	PO5 – Administrar la inversión de TI
	PO6 – Comunicar las aspiraciones y la dirección de la Gerencia
	PO7 – Administrar recursos humanos de TI
	PO8 – Administrar la calidad
	PO9 – Evaluar y administrar los riesgos de TI
	PO10 – Administrar proyectos
Dominio 2 Adquirir e implementar (AI)	AI1 – Identificar soluciones automatizadas
	AI2 – Adquirir y mantener software aplicativo
	AI3 – Adquirir y mantener infraestructura tecnológica
	AI4 – Facilitar la operación y el uso
	AI5 – Adquirir recursos de TI
	AI6 – Administrar cambios
	AI7 – Instalar y acreditar soluciones y cambios
Dominio 3 Entregar y dar soporte (DS)	DS1 – Definir y administrar los niveles de servicio
	DS2 – Administrar los servicios de terceros
	DS3 – Administrar el desempeño y la capacidad
	DS4 – Garantizar la continuidad del servicio
	DS5 – Garantizar la seguridad de los sistemas
	DS6 – Identificar y asignar costos
	DS7 – Educar y entrenar a los usuarios
	DS8 – Administrar la mesa de servicio y los incidentes
	DS9 – Administrar la configuración
	DS10 – Administrar los problemas
	DS11 – Administrar los datos

	DS12 – Administrar el ambiente físico
	DS13 – Administrar las operaciones
Dominio 4 Monitorear y evaluar (ME)	ME1 – Monitorear y evaluar el desempeño de TI
	ME2 - Monitorear y evaluar el control interno
	ME3 – Garantizar el cumplimiento regulatorio
	ME4 – Proporcionar gobierno de TI

A cada uno de estos objetivos se le asigna un nivel de Madurez que es definido por COBIT en forma precisa, lo que permite a la dirección tomar las medidas necesarias para mejorar la situación existente y planificar las acciones a futuro para alcanzar el nivel deseado por la organización.

Si bien cada objetivo de control tiene su modelo de nivel de madurez propio, existe un modelo genérico aplicable a todos ellos definido de la siguiente forma:

0 - No Existente: Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

1 - Inicial: Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo, no se encuentran definidos procesos estándar y en su lugar se utilizan enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2 - Repetible: Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3 – Definido: Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar o no estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados, pero formalizan las prácticas existentes.

4 – Administrado: Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

5 – Optimizado: Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Mediante la aplicación de esta metodología un auditor puede determinar cuál es el grado de madurez en cada uno de los objetivos de control para indicarle a la Dirección dónde hacer foco con el fin de mejorar el gobierno de TI de la organización. Permite también expresar recomendaciones puntuales sobre cada tema evaluado.

7.3.2 COBIT 5

ISACA publicó en abril de 2012 una nueva versión de su marco de trabajo, llamada COBIT 5. Se basa en COBIT 4.1, y toma en cuenta otros marcos como Val IT y Risk IT, *Information Technology Infrastructure Library* (ITIL) y las normas ISO relacionadas en esta norma (Information Systems Audit and Control Association, 2012).

Esta nueva versión da un marco integral de trabajo para que las organizaciones alcancen los objetivos de gobierno de TI que las mismas se hayan propuesto. Permite crear el valor óptimo de TI, minimizando los factores de riesgo y optimizando el uso de los recursos.

Al igual que la versión anterior, es un modelo genérico que puede aplicarse a organizaciones de cualquier tamaño y actividad.

Este modelo se basa en cinco principios claves:

1-. Satisfacer las necesidades de las partes interesadas.

2-. Cubrir la empresa de extremo a extremo.

3-. Aplicar un marco de referencia integrado.

4-. Hacer posible un enfoque holístico.

5.- Separar al gobierno de la gestión.

Con respecto a esto último COBIT 5 define:

- Gobierno: es la función propia del directorio que se ocupa de crear las condiciones para alcanzar las metas propuestas de la organización.

- Gestión: es la función que verifica que se realicen las tareas necesarias para cumplir con las metas establecidas por la organización. Es responsabilidad de la dirección ejecutiva.

COBIT 5 utiliza el mecanismo de Cascada de Metas para que, a partir de las metas corporativas, se establezcan metas específicas en cada uno de los niveles a fin de cumplir con lo definido por el directorio. Este método permite también asignar prioridades en las tareas a realizar para mejorar el gobierno de TI de la organización.

COBIT 5 es una version superadora de las anteriores versiones de COBIT e integra además otros productos y estudios desarrollados por ISACA tales como Val IT, Risk IT, BMIS (*Business Model for Information Security* – Modelo de Negocio para la Seguridad de la nformación) , la publicación *Board Briefing on IT Governance*, entre otros.

Esta metodología utiliza elementos llamados catalizadores, los cuales influyen en el gobierno y en la gestión de TI. Se definen siete categorías de catalizadores:

- Principios, políticas y marcos de referencia.
- Procesos.
- Estructuras organizativas.
- Cultura ética y comportamiento.
- Información.
- Servicios, infraestructura y aplicaciones.
- Personas, habilidades, y competencias.

COBIT 5 divide los procesos en dos dominios, uno de gobierno y otro de gestión empresarial.

Los procesos de gobierno tienen como principales funciones las de evaluar, orientar y supervisar (EDM. *Evaluate, Direct and Monitor*), y este modelo los define de la siguiente forma:

EDM01 – Asegurar el establecimiento y mantenimiento del marco de gobierno.

EDM02 – Asegurar la entrega de beneficios.

EDM03 – Asegurar la optimización del riesgo.

EDM04 – Asegurar la optimización de recursos.

EDM05 – Asegurar la transparencia hacia las partes interesadas.

Los procesos de gestión pueden clasificarse de acuerdo a la siguiente tabla:

Tabla 2 - Modelo COBIT 5

Alinear, planificar y organizar (APO)	APO01 – Gestionar el marco de gestión de TI
	APO02 – Gestionar la estrategia
	APO03 – Gestionar la arquitectura empresarial
	APO04 – Gestionar la innovación
	APO05 – Gestionar el portafolio
	APO06 – Gestionar el presupuesto y los costes
	APO07 – Gestionar los recursos humanos
	APO08 – Gestionar las relaciones
	APO09 – Gestionar los acuerdos de servicio
	APO10 – Gestionar los proveedores
	APO11 – Gestionar la calidad
	APO12 – Gestionar el riesgo
	APO13 – Gestionar la seguridad
Construir, adquirir e implementar (BAI)	BAI01 – Gestionar programas y proyectos
	BAI02 – Gestionar la definición de requisitos
	BAI03 – Gestionar la identificación y construcción de soluciones
	BAI04 – Gestionar la disponibilidad y la capacidad
	BAI05 – Gestionar la introducción del cambio organizativo
	BAI 06 – Gestionar los cambios
	BAI07 – Gestionar la aceptación del cambio y la transición
	BAI08 – Gestionar el conocimiento
	BAI09 – Gestionar los activos
	BAI10 – Gestionar la configuración
Entrega, servicio y soporte (DSS)	DSS01 – Gestionar operaciones
	DSS02 – Gestionar peticiones e incidentes de servicio
	DSS03 – Gestionar problemas

	DSS04 – Gestionar la continuidad
	DSS05 – Gestionar servicios de seguridad
	DSS06 – Gestionar controles de proceso de negocio
Supervisar, evaluar y valorar (MEA)	MEA01 – Supervisar, evaluar y valorar el mantenimiento y la conformidad
	MEA02 – Supervisar, evaluar y valorar el sistema de control externo
	MEA03 – Supervisar, evaluar y valorar la conformidad con los requerimientos externos

Esta metodología utiliza como métrica la llamada Niveles de Capacidad de Proceso, que está basada en la norma ISO/IEC 15504. Los niveles definidos son:

- Nivel 0 – Proceso Incompleto: El proceso no está implantado o no alcanza sus objetivos.
- Nivel 1 – Proceso Ejecutado: El proceso implantado alcanza su objetivo.
- Nivel 2 – Proceso Gestionado: El proceso es implantado de forma planificada, supervisada y ajustada. Sus resultados son debidamente establecidos, controlados y mantenidos.
- Nivel 3 – Procesos Establecidos: El proceso se implementa siguiendo un procedimiento definido para alcanzar su objetivo.
- Nivel 4 - Proceso Predecible: El proceso es operado dentro de límites definidos para alcanzar sus resultados.
- Nivel 5 – Proceso Optimizado: El proceso es mejorado continuamente para alcanzar las metas de negocio actuales y futuras.

7.3.3 CMMI

Capability Maturity Model Integration – Integración de modelos de madurez de capacidades (CMMI), es un modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software. Fue desarrollado por el *Software Engineering Institute* (SEI) de la *Carnegie Mellon University*, patrocinado por el Departamento de Defensa de EUA.

Fue desarrollado inicialmente para mejorar la capacidad de los procesos relativos al desarrollo e implementación de software.

Tiene como base estudios realizados por IBM y el *Manufactoring Maturity Model* del Philip Crosby.

El marco CMMI proporciona la estructura necesaria para crear los modelos, la formación y los componentes de evaluación de CMMI. Para permitir el uso de múltiples modelos dentro del marco CMMI, los componentes de los modelos se clasifican como comunes a todos los modelos CMMI o aplicables a un modelo específico. El material común se denomina "*CMMI Model Foundation*" o "*CMF*." Los componentes del CMF son parte de todos los modelos generados a partir del marco CMMI. Esos componentes se combinan con el material aplicable a un área de interés (por ejemplo, adquisición, desarrollo, servicios) para crear un modelo. Una "constelación" se define como una colección de componentes CMMI que se usan para construir modelos, materiales de formación y documentos relativos a la evaluación para un área de interés (por ejemplo, adquisición, desarrollo, servicios). El modelo de la constelación de desarrollo se denomina "CMMI para Desarrollo" o "CMMI-DEV" (Software Engineering Institute, 2010).

Éste consiste en un conjunto de buenas prácticas que tratan las actividades de desarrollo aplicadas a productos y servicios. Se ocupa de las prácticas que cubren el ciclo de vida del producto desde la concepción hasta la entrega y el mantenimiento.

El SEI, en sus investigaciones para ayudar a las organizaciones a desarrollar y mantener productos y servicios de calidad, ha identificado varias dimensiones en las que una organización puede centrarse para mejorar su actividad.

De acuerdo a esta metodología existen tres dimensiones críticas donde normalmente se centran las organizaciones: las personas, los métodos y procedimientos, y el equipamiento y herramientas. Todos estos elementos se vinculan entre sí a través de los procesos.

El SEI se basa en la premisa de la gestión de procesos, la calidad de un sistema o producto y la calidad del proceso empleado para desarrollarlo y mantenerlo, para definir diversos CMMs para la mejora de distintos procesos.

Éstos contienen los elementos esenciales de los procesos eficaces de una o más disciplinas y permiten una evolución ordenada para la mejora desde procesos *ad hoc* e inmaduros a procesos maduros de mayor calidad y eficacia.

7.3.4 ITIL

ITIL (*IT Infrastructure Library*, Biblioteca de infraestructura de TI) es un marco de referencia que indica las buenas prácticas para la administración de servicios de TI, con un enfoque de administración de procesos.

Desarrollado durante los años 1980, ITIL no fue ampliamente adoptada sino hasta mediados de los años 90. Esta mayor difusión lo llevó a ser utilizado en la creación de varios estándares, como por ejemplo ISO/IEC 20000, que toma los elementos de gestión de servicios de TI de ITIL

Se lo utiliza muchas veces junto con otros marcos de trabajo de mejores prácticas como la *Information Services Procurement Library* (ISPL, 'Biblioteca de adquisición de servicios de información'), la *Application Services Library* (ASL, 'Biblioteca de servicios de aplicativos'), el método de desarrollo de sistemas dinámicos (DSDM, *Dynamic Systems Development Method*), el Modelo de Capacidad y Madurez (CMM/CMMI) y también con la gobernanza de tecnologías de la información mediante COBIT (*Control OBjectives for Information and related Technology*). La Gestión de Servicio ITIL está actualmente integrado en el estándar ISO 20000 (anterior BS 15000).

ITIL se construye en torno a una vista basada en proceso-modelo del control y gestión de las operaciones. Sus recomendaciones fueron desarrolladas en los años 1980 por la *Central Computer and Telecommunications Agency* (CCTA) del gobierno británico como respuesta a la creciente dependencia de las tecnologías de la información y al reconocimiento de que sin prácticas estándar, los contratos de las agencias estatales y del sector privado creaban independientemente sus propias prácticas de gestión de TI y duplicaban esfuerzos dentro de sus proyectos TI, lo que resultaba en errores comunes y mayores costos.

ITIL fue publicado como un conjunto de libros, cada uno dedicado a un área específica dentro de la Gestión de TI. Los nombres ITIL e *IT Infrastructure Library* ('Biblioteca de infraestructura de TI') son marcas registradas de la *Office of Government Commerce* ('Oficina de comercio gubernamental', OGC), que es una división del Ministerio de Hacienda del Reino Unido.

En diciembre de 2005, la OGC emitió un aviso de una actualización a ITIL 2 conocida comúnmente como ITIL v3, que estuvo planificada para ser publicada a finales de 2006 pero que recién salió en junio de 2007. Esta versión de ITIL incluye cinco

libros principales: Diseño de Servicios de TI, Introducción de los Servicios de TI, Operación de los Servicios de TI, Mejora de los Servicios de TI y Estrategias de los Servicios de TI, consolidando buena parte de las prácticas actuales de la versión 2 en torno al Ciclo de Vida de los Servicios.

ITIL busca mejorar la calidad, entendiéndose que la misma se alcanza cuando el cliente recibe todas las características que exige de un servicio o producto. La Gestión de la Calidad es todo lo que la organización realiza para garantizar que se satisfacen los requisitos de los clientes y se cumplen todas las normas aplicables.

La gestión de la calidad de los servicios de TI tiene que garantizar que la información es confiable y segura.

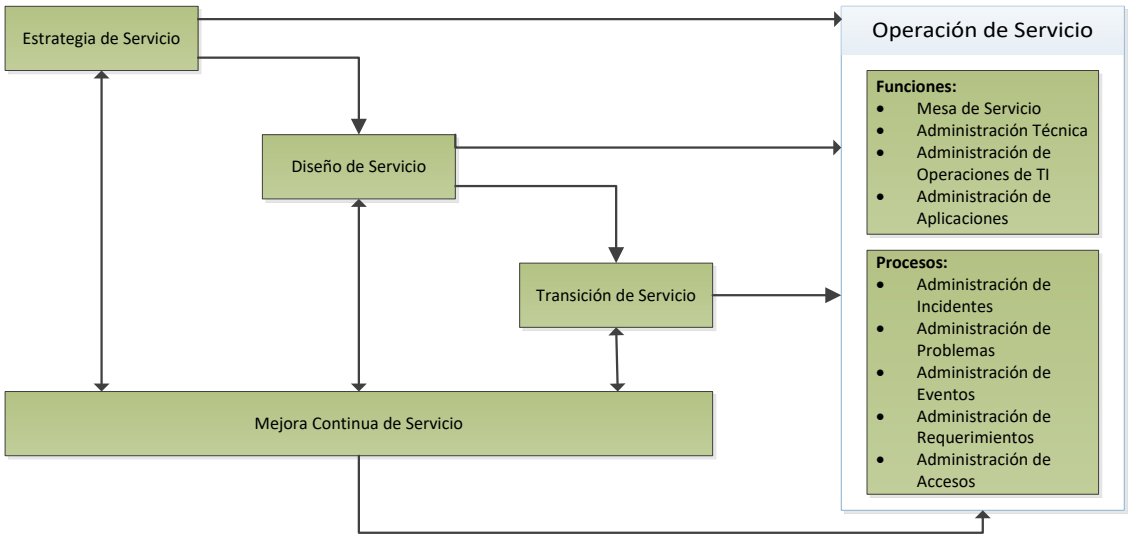
La gestión de los servicios de TI consiste en administrar todos los procesos para garantizar la calidad de los servicios de TI en producción, de acuerdo con los niveles de servicio acordados con el cliente.

ITIL es una biblioteca que documenta las buenas prácticas de Gestión de TI, sus cuatro principios o pilares son:

1. Procesos.
2. Calidad.
3. Cliente.
4. Independencia

El mapa de procesos de ITIL es:

Ilustración 2 - Mapa de Procesos de ITIL



Fuente: Elaboración propia

Esta metodología define los siguientes elementos:

- Alerta: Advertencia de que se ha superado un umbral, que se produjo un cambio o un fallo.
- Evento: Cambio de estado significativo en un elemento de configuración o un servicio de TI.
- Fallo: Pérdida de la habilidad de la operar de acuerdo a las especificaciones o de proporcionar el resultado requerido.
- Incidente: Interrupción no planificada de un servicio de TI o reducción en su calidad.
- Problema: Causa desconocida de uno o más incidentes.
- Impacto: Medida del efecto de un incidente, problema o cambio en los procesos del negocio.
- Urgencia: Medida del efecto de un incidente, problema o cambio que provocará un impacto significativo para el negocio.
- Prioridad: Identificación de la importancia relativa de un incidente, problema o cambio, es función del impacto y la urgencia.
- Solución temporal (*workaround*): Reducción o eliminación del impacto de un incidente o problema para el que la solución definitiva aún no está disponible.

ITIL establece las relaciones de la gestión de niveles de servicio:

- Gestión de incidencias: se ocupa de procesar y restablecer la operación normal del servicio tan pronto como sea posible, minimizando el impacto adverso en el negocio.
- Gestión de problemas: se ocupa proactivamente de prevenir fallos que puedan causar incidentes en la infraestructura y reactivamente buscando las causas de las incidencias.
- Gestión del cambio: asegura que los cambios se realizan de una forma controlada, evaluada, priorizada, planificada, probada y documentada.
- Gestión de proveedores: se encarga de administrar las relaciones con proveedores y su desempeño.
- Gestión de la disponibilidad: se ocupa de asegurar que los niveles de servicio acordados de disponibilidad se estén cumpliendo.
- Gestión de la capacidad: se ocupa de los temas de capacidad y rendimiento.
- Gestión de la seguridad de la información: se encarga de proteger los sistemas y las comunicaciones encargadas de suministrar la información.
- Mejora continua del servicio.

7.3.5 IRAM – ISO – IEC 17799

El Instituto Argentino de Normalización (IRAM) es el representante en Argentina de la *International Organización for Standardization* (ISO) y como tal adopta las normas publicadas por ésta como propias.

Esta norma establece los principios generales para implementar y mantener la gestión de la información de una organización. Está pensada para implementar controles en debilidades identificadas después de un análisis de riesgo.

Establece una serie de definiciones con el fin de establecer un vocabulario común para evitar confusiones en la descripción de los controles.

Este estándar tiene 11 cláusulas de control de seguridad, las cuales contienen un total de 39 categorías de seguridad principales (Instituto Argentino de Normalización y Certificación, 2005). Estas cláusulas son:

a) Política de Seguridad.
b) Organización de la Seguridad de la Información.
c) Gestión de Activos.

d) Seguridad de Recursos Humanos.

e) Seguridad Física y Ambiental.

f) Gestión de Comunicaciones y Operaciones.

g) Control de Acceso.

h) Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

i) Gestión de Incidentes de Seguridad de Información.

j) Gestión de la Continuidad Comercial.

k) Conformidad.

Cada categoría de seguridad contiene un objetivo de control que establece lo que debe lograr y uno o más controles a aplicar para logarlo.

7.3.6 ISO 27001

Modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad Informática (SGSI) (Information Security Management System, ISMS).

A través de esta norma se busca establecer una implementación efectiva de la seguridad de la información empresarial.

Como antecedente de esta norma, se puede mencionar la norma BS 7799, de la *British Standars Institution* (BSI), cuyo objetivo era la de adecuar a una empresa para certificar su gestión de la seguridad de la información por medio de una auditoría externa realizada por un auditor certificado. Esta norma consta de dos partes, la primera es una guía de buenas prácticas que no establece un modelo de certificación, la segunda certifica a aquellas organizaciones que hayan desarrollado un Sistema de Gestión de Seguridad de la Información según el modelo Planificar-Hacer-Verificar-Actuar (PDCA, *Plan-Do-Check-Act*).

Esta norma fue revisada y adoptada por ISO como ISO 17799 en el 2000. En 2005 se publica el sistema SGSI (Sistema de Gestión de Seguridad de la Información) bajo la norma ISO 27001.

En su contenido se define cómo se debe establecer, implementar, mantener y mejorar un SGSI, cómo se documenta el mismo y cómo se lo controla. Además, define cómo se deben realizar las auditorías internas de control y cómo se gestiona el proceso de

revisión. También incluye una tabla de correspondencia con las normas ISO 9001 e ISO 14001 (Instituto Argentino de Normalización y Certificación, 2007).

La norma ISO 27001 está acompañada por otras entre las cuales podemos mencionar:

ISO 27002: es una guía de buenas prácticas que describe los objetivos de control y controles recomendables para la seguridad de la información. Contiene 39 objetivos de control y 133 controles agrupados en 11 dominios.

ISO 27005: establece directrices para la gestión de riesgo en la seguridad de la información.

ISO 27006: especifica los requisitos que deben cumplir las organizaciones dedicadas a la auditoría y la certificación de sistemas de gestión de seguridad de información.

7.3.7 Norma ANSI TIA 942

Esta norma dictada por la *American National Standards Institute (ANSI)* y por la *Telecommunications Industry Association* (TIA), clasifica un centro de procesamiento de datos (data center) en cuatro niveles de acuerdo a la redundancia de sus sistemas, principalmente de suministro eléctrico y comunicaciones.

Las principales características de cada uno de los niveles son:

Nivel 1: Básico – Tiene rutas únicas, no tiene componentes redundantes. Esto lo deja vulnerable frente a interrupciones planeadas y no planeadas. Los errores de operación o fallas espontáneas de los componentes de infraestructura provocan interrupciones en el servicio del centro de cómputos.

Nivel 2: Componentes redundantes – Son menos vulnerables a las interrupciones que los de Nivel 1. El diseño de UPS y generadores alternativos debe tener una redundancia de N+1, pero sólo con un camino de distribución, por lo tanto, para una reparación de la ruta de distribución eléctrica es necesario interrumpir el servicio del data center.

Nivel 3: Permite hacer mantenimientos sin interrupciones - Cuenta con:

- Rutas múltiples.
- Sistema multimódulo.
- Doble ruta de alimentación eléctrica de potencia.

- Pérdida de redundancia durante falla o mantenimiento.

Permite realizar actividades de mantenimiento planeadas sin tener que interrumpir el servicio. No queda redundancia durante la realización de estos trabajos. Permite elevar a Nivel 4 fácilmente.

Nivel 4: Tolerante a fallas – Cuenta con:

- Múltiples rutas.
- Componentes redundantes.
- Fuente dual de potencia crítica.
- No hay pérdida de redundancia durante trabajos de mantenimiento.

Da seguridad que no se produzcan interrupciones en el servicio ya sea por actividades de mantenimiento planeadas o no. Sólo debería tener una salida de servicio ante la activación del sistema de apagado de emergencia.

Sobre este tema, existen también las normas dictadas por ICREA *(International Computer Room Experts Association*) que define los niveles de acuerdo al porcentaje de disponibilidad en horas al año que el centro de cómputos puede estar fuera de servicio.

Ésta divide a los data centers en cinco categorías (International Computer Room Experts Association, 2017):

Tabla 3 - Niveles de servicio - ICREA

Nivel	Descripción	Disponibilidad
I	Quality assurance data center (QADC)	95%
II	World class quality assurance data center (WCQA)	99%
III	Safety world class quality assurance data center (S - WCQA)	99.90%
IV	High security world class quality assurance data center (HS - WCQA)	99.99%
V	High security high available world class quality assurance data center (HSHA - WCQA)	100%

Fuente: ICREA

7.3.8 PMBOK

El PMI (*Project Management Institute*) es una asociación de profesionales dedicados a la gerencia de proyectos que se ocupan de promover el desarrollo del conocimiento y las competencias básicas para el ejercicio de la profesión.

PMBOK (*Project Management Body of Knowledge*) es una guía desarrollada por el PMI con el fin de brindar pautas para la dirección de proyectos.

Esta metodología permite definir el ciclo de vida de un proyecto y, asociado a éste, el ciclo de vida de la dirección de proyectos. Presenta un estándar reconocido internacionalmente que describe normas, métodos y procesos.

El documento principal es la Guía del PMBOK (*PMBOOK's Guide*), la cual presenta al comienzo una visión general y después brinda definiciones respecto a qué es un Proyecto, qué es la Dirección de Proyectos, cuáles son las relaciones entre la dirección de Proyectos y la Dirección Organizacional de Proyectos, cómo se define el Valor del Negocio, entre otras (Project Management Institute, Inc., 2013).

7.3.9 Auditoría de Valor (Audit for Value)

La NAO (National Audit Office) utiliza tres criterios para describir el valor monetario de los gastos gubernamentales, por ejemplo, el uso óptimo de los recursos para lograr las metas deseadas. Estos son:

1. Economía: minimizar el costo de los recursos utilizados o requeridos (gastar menos).
2. Eficiencia: la relación entre la salida de bienes o servicios y los recursos utilizados para producirlos (gastar bien).
3. Efectividad: la relación entre los resultados deseados del gasto público y los realmente obtenidos (gastar inteligentemente).

Existe un cuarto criterio que se aplica en determinados casos, éste es:

4. Equidad: el alcance y disponibilidad del servicio deben alcanzar a la población para la cual el mismo fue diseñado (gastar equilibradamente).

Mediante esta metodología un organismo de control gubernamental puede analizar el uso de los recursos públicos.

7.4 Competencia

El producto a desarrollar, un Manual de Auditoría de TI para la AGN, tiene un grado de especificidad tan alto que no existen en el mercado otros que puedan reemplazarlo en forma directa. La principal barrera para ello es el cumplimiento estricto de leyes nacionales y reglamentaciones internas propias de la AGN.

A pesar de esto existen algunos manuales de entidades gubernamentales que podrían ser adaptados para ser utilizados por la AGN. Como ejemplo de éstos podemos mencionar a:

- Normas de Control Interno para Tecnologías de la Información de la Sindicatura General de la Nación de la República Argentina.
- Manual del Auditoría Gubernamental de la Contraloría General de Cuentas de Guatemala.
- Manual de Auditoría Financiera Gubernamental de la Contraloría General del Estado de la República de Ecuador.
- Normas de Auditoría Gubernamental de la Contraloría General de la República de Nicaragua.
- Normas Brasileiras de Auditoría do Setor Público (NBASP) del Tribunal de Contas da União.

8. Diseño Metodológico

En este punto se describe cuáles serán los métodos, herramientas y procedimientos que se utilizarán en el desarrollo del trabajo.

En la etapa de relevamiento se utilizarán:

- Entrevistas no estructuradas con preguntas abiertas al personal del Departamento de Auditoría Informática de la AGN.
- Análisis de la normativa existente tanto a nivel nacional como internacional referida al control de los distintos aspectos de TI.
- Análisis de los informes de auditoría realizados por el Departamento de Auditoría Informática.

Una vez realizadas las tareas de relevamiento, se comenzará con la redacción propia del manual de auditoría. Éste será desarrollado en distintas etapas, donde cada una

de ellas tendrá como entregable el capítulo correspondiente del manual. En principio estos capítulos son:

1. Introducción. Visión general. Objetivos
2. Marco de referencia de las auditorías de TIC.
3. Planeamiento del trabajo de auditoría.
4. Ejecución del trabajo de auditoría.
5. Seguimiento de las recomendaciones de los informes.
6. Apéndices.

Los Apéndices tratarán sobre temas particulares y en su contenido se especificarán los procedimientos detallados a realizar, que serán evidencia de los hallazgos de auditoría. Dentro de éstos podemos mencionar:

- Planificación y organización del área de TIC.
- Desarrollo de aplicaciones.
- Seguridad perimetral. Configuración de Antivirus, Firewalls y DMZ (demilitarized zone – zona desmilitarizada)
- Administración de usuarios
- Seguridad física.

Entre otros.

9. Relevamiento

9.1 Relevamiento estructural

La AGN dispone de 2 edificios propios en la zona de Congreso en la Ciudad Autónoma de Buenos Aires.

En el edificio principal se encuentran las oficinas de los Auditores Generales, sus asesores, la Gerencia de Administración y Finanzas, y algunas de las gerencias sustantivas (son aquellas que realizan tareas directas de auditoría). En el segundo edificio se encuentran las oficinas del resto de las gerencias sustantivas.

Debe tenerse en cuenta que gran parte del personal de la AGN realiza tareas de campo en distintos organismos del SPN, por lo tanto, efectúan sus actividades en las oficinas de los entes que están bajo auditoría.

La AGN cuenta con un centro de cómputos ubicado en el edificio principal. En él se alojan los servidores que soportan las aplicaciones corporativas. Entre ellas se pueden mencionar:

- Sistema de Administración de Usuarios.
- Sistema de Administración de RR.HH. y Liquidación de Sueldos.
- Sistema de Control de Auditorías.
- Sistema de Legajo Permanente de Organismos.
- Sistema de Seguimiento de Expedientes.
- Correo Corporativo.
- Sistema de Consulta de Normas Internas (DIGESTO).
- Sistema de Solicitud de Requerimientos.
- Página Web de la AGN.
- Intranet del Organismo.
- ACL (Aplicación para el análisis de bases de datos).

Entre otros.

Además, se cuenta con un File Server que permite, por un lado, compartir archivos entre los empleados de un mismo Departamento, y por otro, que cada agente almacene sus archivos personales de trabajo a los que sólo él tiene acceso.

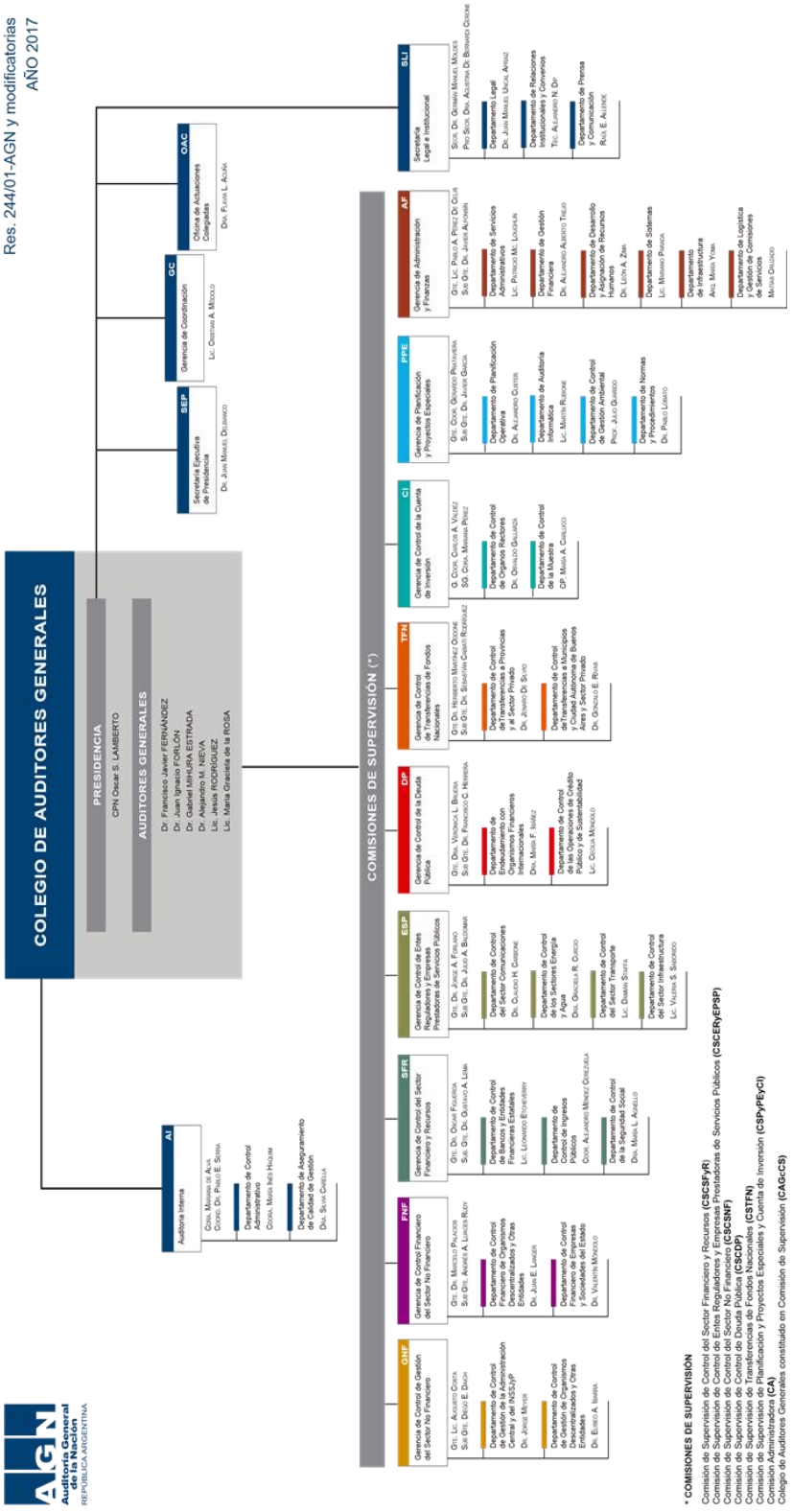
Los empleados que se encuentran realizando tareas de auditoría en los distintos organismos utilizan notebooks suministradas por la AGN o computadoras personales que suministra el organismo auditado. En este caso, los agentes que necesiten disponer de los recursos informáticos que se encuentran en las oficinas centrales de la AGN lo pueden hacer a través de la Web accediendo a la intranet utilizando su nombre de usuario y clave de acceso.

9.2 Relevamiento funcional

9.2.1 Organigrama

El organigrama de toda la AGN (Auditoría General de la Nación, 2017) es el siguiente:

Ilustración 3 - Organigrama de la AGN



Fuente: https://www.agn.gov.ar/files/files/organigrama.pdf

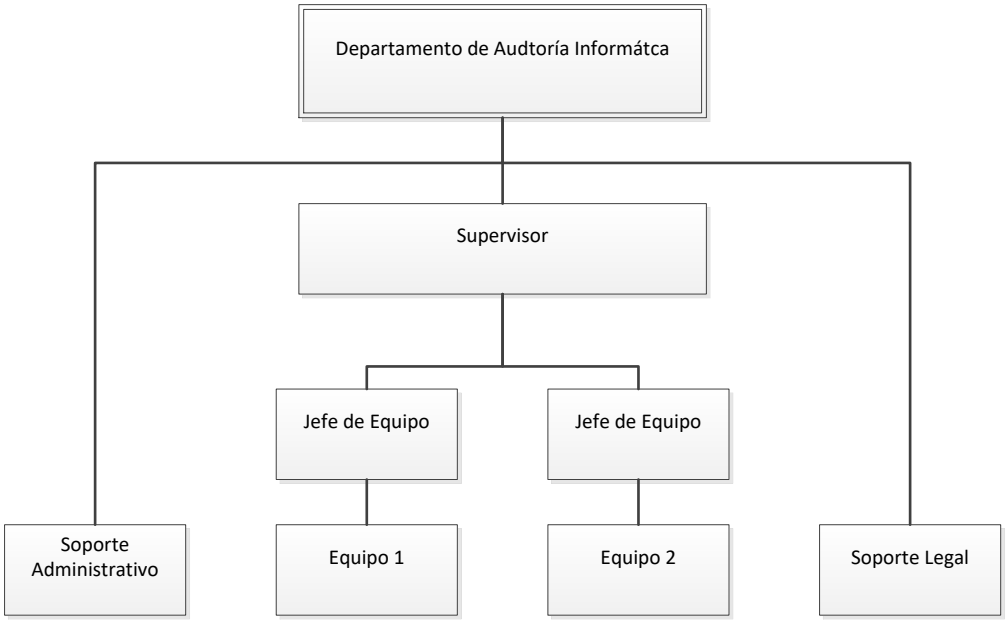
A continuación, se lo detalla con más precisión, haciendo foco en la rama en que se encuentra ubicado el Departamento de Auditoría Informática.

Ilustración 4 - Organigrama de la AGN parcial

Fuente: Elaboración propia

La organización del Departamento de Auditoría Informática es la siguiente:

Ilustración 5 - Organigrama del Departamento de Auditoría Informática



Fuente: Elaboración propia

9.2.2 Funciones de las áreas

Del análisis de los organigramas mostrados en el punto anterior podemos mencionar:

- Colegio de Auditores Generales: Como se mencionó en el punto 7.1 de este trabajo, es la máxima autoridad del organismo. Está formado por un presidente elegido por el partido de la oposición con mayor representación parlamentaria, y por seis Auditores Generales, elegidos tres por la Cámara de Senadores y tres por la Cámara de Diputados respetando la proporción de mayorías y minorías de cada cámara. Entre sus funciones se encuentran las de aprobar la planificación anual que indica cuáles serán las auditorías a realizar y de aprobar formalmente cada una de las auditorías finalizadas.
- Comisión de Supervisión: Se encarga de dar la aprobación para el inicio de la auditoría mediante la apertura de la actuación administrativa correspondiente, gestionar toda la comunicación formal que se establezca entre la AGN y el organismo auditado, y efectuar el control de la auditoría mientras la misma se realiza. Una vez terminado el trabajo, esta comisión emite un dictamen para que sea tratado por el Colegio de Auditores Generales para su aprobación final.
- Gerencia de Planificación: dentro de sus responsabilidades se encuentra la de: "*... Planificar y dirigir las auditorías y exámenes tendientes a evaluar la gestión informática del Estado Nacional*". Dentro de sus acciones se encuentra la de "*...Considerar en cada caso el informe del Auditor actuante, la opinión del Jefe de Departamento competente y elaborar y suscribir, cuando corresponda, el dictamen definitivo*" (Auditoría General de la Nación, 2008).
- Departamento de Auditoría Informática: tiene como responsabilidad primaria "*Programar, coordinar, supervisar y ejecutar las acciones necesarias para evaluar, en el Sector Público Nacional, la consistencia, compatibilidad, integridad y seguridad de los sistemas informáticos, la calidad, actualidad y legalidad de la tecnología de información utilizada. Brindar asistencia en materia de auditoría de sistemas de información y de contrataciones de bienes, insumos, servicios informáticos y comunicaciones asociadas*". Para ello dentro de sus acciones se encuentran las de: i) "*Efectuar relevamientos en los organismos del Sector Público Nacional competentes en los aspectos de definición de política informática de la Administración Pública Nacional en cuanto al ejercicio de tales*

funciones.", ii) "*Intervenir en la elaboración de convenios entre la Auditoría General de la Nación e instituciones públicas o privadas especializadas en el ámbito de su incumbencia*", iii) "*Elaborar la planificación específica de las auditorías y exámenes y someter el proyecto a la aprobación de la Gerencia*", entre otras (Auditoría General de la Nación, 2004).

- Supervisor: las funciones del supervisor son las de ejercer *"... funciones de organización y control de unidades organizativas dependientes denominadas EQUIPOS DE AUDITORÍA, que desempeñen actividades de control. Esta tarea supone coordinar y supervisar el cumplimiento de los procesos y las relaciones entre los equipos a su cargo, así como el cumplimiento de las responsabilidades encomendadas a los jefes y equipos bajo su supervisión*" (Auditoría General de la Nación, 2004).
- Jefe de Equipo: sus funciones son las de ejercer "*... las funciones de control operativo de las unidades organizativas denominadas EQUIPOS DE AUDITORÍA, que desempeñen actividades de control. Esta tarea supone la responsabilidad sobre el cumplimiento de las tareas y objetivos del equipo a su cargo*" (Auditoría General de la Nación, 2004).
- Equipo de Auditoría: se encarga de realizar las tareas de auditoría de campo. Entre ellas podemos mencionar la recolección y análisis de la evidencia obtenida, entrevistas con los responsables de las distintas áreas, inspecciones oculares de las instalaciones, entre otras.
- Soporte Legal: es un abogado que se ocupa de brindar apoyo a los equipos de auditoría en temas de su competencia, como por ejemplo el marco legal y normativo de los organismos auditados, y los aspectos legales de los contratos que los mismos celebran con distintos proveedores.
- Soporte Administrativo: se ocupa de la gestión administrativa del Departamento, las notas entrantes y salientes, llevar el control de la asistencia del personal, el manejo de los insumos de oficina, entre otros temas.

El área de auditoría informática se creó informalmente ante la necesidad de realizar este tipo de trabajos, hasta que en el 2001 se formalizó como parte del Departamento de Sistemas, pasando éste a denominarse Departamento de Auditoría Informática y Sistemas. Esta unidad tuvo como principal inconveniente problemas de

gestión derivados de la gran diferencia que existe entre la realización de trabajos de auditoría externa y el manejo de un área operativa de sistemas. Por este motivo, en el año 2004 se separaron ambas funciones creándose dos departamentos, el de Sistemas por un lado y el de Auditoría Informática por el otro.

Dentro de los trabajos realizados por el Departamento de Auditoría Informática se pueden mencionar auditorías de gestión de TIC a organismos tales como Administración Federal de Ingresos Públicos, Administración Nacional de Servicios de la Seguridad Social, Instituto Nacional de Servicios Sociales para Jubilados y Pensionados, Dirección General de Aduanas, Subsecretaría de Pesca y Acuicultura, Registro Nacional de Dominios de Internet, entre otros.

Cabe destacar que, a diferencia de la mayoría de los trabajos de auditoría, tanto interna como externa, los informes que realiza la AGN son públicos a fin dar transparencia al control que se realiza a los organismos del SPN. Todos los informes producidos pueden ser consultados en la página web de la AGN (www.agn.gov.ar).

Desde su creación, el Departamento de Auditoría Informática conformó dos equipos de trabajo fijos. Uno de ellos se dedicó a realizar auditorías de gestión de TIC utilizando como plantilla de trabajo el estándar COBIT v2, y para ello confeccionó documentación precisa, en forma de cuestionarios y listas de verificación que permitían un trabajo uniforme en las auditorías que se realizaban a los distintos organismos. Por otra parte, el otro equipo de trabajo se abocó a efectuar auditorías sobre temas específicos utilizando una metodología *ad hoc* en cada caso.

Con el transcurso del tiempo el equipo de auditoría que utilizaba COBIT evolucionó a la versión 3, dado que los cuestionarios de la versión 2 habían quedado tecnológicamente desactualizados al no haberse realizado las tareas necesarias de adecuación de los mismos y por ello se dejaron de usar. En su lugar se desarrolló una aplicación llamada SIATI (Sistema de Auditorías de Tecnologías de la Información), programado en ORACLE Forms, y utilizando como motor de base de datos a ORACLE. Este sistema permitía seleccionar los niveles de madurez para cada uno de los puntos de control de alto nivel, y redactar las observaciones correspondientes. Si bien era un desarrollo interesante, SIATI no tuvo éxito básicamente por dos motivos: el primero, que su interfaz era muy poco amigable con el usuario; y el segundo, que no realizaba correctamente la exportación a MS – Word obligando a un trabajo adicional de corrección

del informe de auditoría, previo a ser elevado a las autoridades para su evaluación, que muchas veces resultaba largo y demoraba la finalización del trabajo.

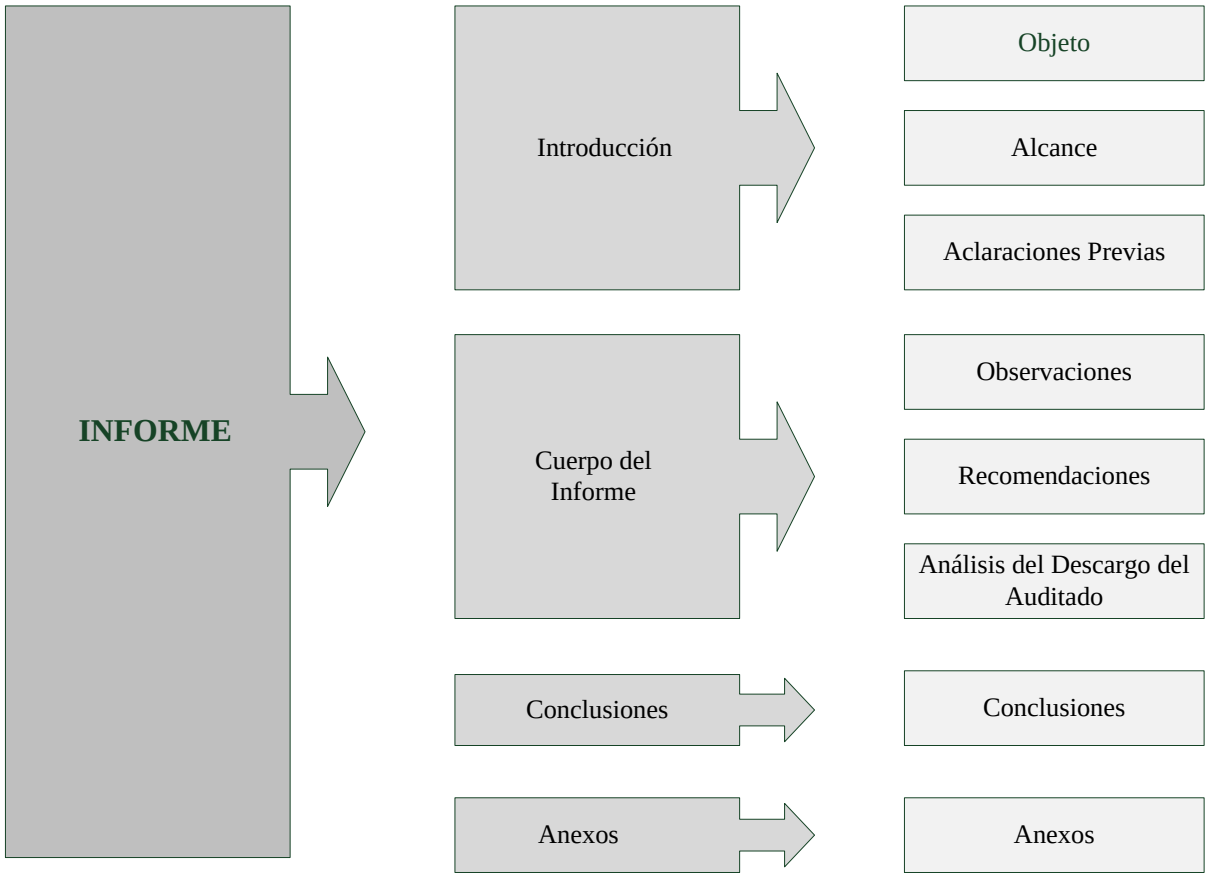
Con la aparición de COBIT 4 se comenzó a utilizar esta versión, siempre como plantilla de trabajo, y se dejó de usar definitivamente el SIATI. Este sistema no fue reemplazado por otro, ni tampoco se generó ninguna metodología definida para la realización de las auditorías, quedando los procedimientos a realizar bajo el criterio del equipo de auditoría actuante.

Desde el año 2016, producto de cambios organizacionales en la AGN, se comenzó con un trabajo de reingeniería que abarca desde la planificación de las auditorías hasta la redacción de los informes. Los cambios efectuados hasta la fecha producto de estos análisis no son realizados siguiendo un proyecto definido de mejoras sino son iniciativas puntuales sobre temas específicos.

Actualmente el Departamento de Auditoría Informática se encuentra en una etapa de diseño de procesos que unifiquen los conceptos utilizados con el fin de aplicar los mismos procedimientos y criterios en cada una de las auditorías de TIC que se realicen.

El informe de auditoría tiene un formato estándar para todas las auditorías que realiza la AGN. Consta de cuatro partes principales las cuales, a su vez, se dividen en distintas partes tal como lo muestra el siguiente gráfico:

Ilustración 6 - Esquema de Informe de Auditoría



Fuente: Elaboración propia

La AGN aprobó mediante la Resolución N°26/15 - AGN las Normas de Control Gubernamental (Auditoría General de la Nación, 2015), las cuales comenzaron a aplicarse en forma obligatoria a partir del 1 de enero de 2016. Estas normas definen cuáles son los objetivos del control externo gubernamental, cuál es su ámbito de aplicación y sus características, entre otros puntos. Además, clasifica a los distintos tipos de auditoría gubernamental de la siguiente forma:

1. Control financiero gubernamental.
    a. Auditoría financiera.
    b. Revisión limitada.
    c. Exámenes especiales.
    d. Certificación
2. Control de gestión gubernamental.
    a. Auditorías de gestión.
    b. Auditorías especializadas.

c. Exámenes especiales.

3. Control de cumplimiento gubernamental.

Las normas enumeran cuáles son los principios éticos fundamentales que deben guiar a los auditores gubernamentales. Ellos son:

I. Independencia de criterio.
II. Confidencialidad.
III. Integridad.
IV. Objetividad.
V. Competencia profesional.
VI. Neutralidad política.
VII. Comportamiento profesional.

Estas normas definen también las distintas etapas que comprende el proceso de control externo gubernamental, y las actividades que se deben realizar en cada una de ellas. Finalizan con las indicaciones de cómo debe redactarse el informe, su forma y contenido, y cómo será el control de calidad que se realizará al mismo.

Debe tenerse en cuenta que estas normas son de alto nivel, es decir no entran en detalle de los procedimientos a realizar en cada tipo de auditoría. Algunas áreas de la AGN definieron formalmente procedimientos específicos para las áreas de su competencia, no siendo ese el caso del Departamento de Auditoría Informática, que aún no formalizó los mismos.

Para la redacción de las normas propias del Departamento se utilizarán como marco los estándares más reconocidos en la industria. En el punto siguiente, se da una breve descripción de los mismos.

9.2.3 Procesos de negocios

El proceso sobre el que se va a trabajar es la realización de una auditoría de TIC. En su página web la AGN describe cuál es el proceso completo de una auditoría. El mismo, representado de forma idéntica a como se muestra en la página web, resulta:

Ilustración 7 - Ciclo de Vida de una Auditoría

Fuente: Elaboración propia

La AGN divide todo el proceso de auditoría en cuatro etapas bien definidas:

1. Planificación: abarca desde el inicio de la auditoría hasta la aprobación del Plan trabajo.
2. Ejecución: etapa en la cual se realizan las pruebas de cumplimiento y sustantivas detalladas en el Plan de Trabajo.
3. Informe: comprende la redacción del informe de auditoría, y su correspondiente proceso de aprobación.
4. Seguimiento: posteriormente a la aprobación del informe, y transcurrido un tiempo prudencial para que el auditado pueda implementar las recomendaciones sugeridas, el Colegio de Auditores Generales puede ordenar la realización de una auditoría de seguimiento con el fin de evaluar las implementaciones realizadas. Esta etapa no será tratada en este trabajo.

A continuación, se describen los tres primeros procesos arriba enunciados.

Proceso: Planificación de una Auditoría.

Roles:

Comisión de Supervisión.
Gerente.
Jefe de Departamento.
Supervisor
Jefe de Equipo
Equipo de Auditoría
Auditado.

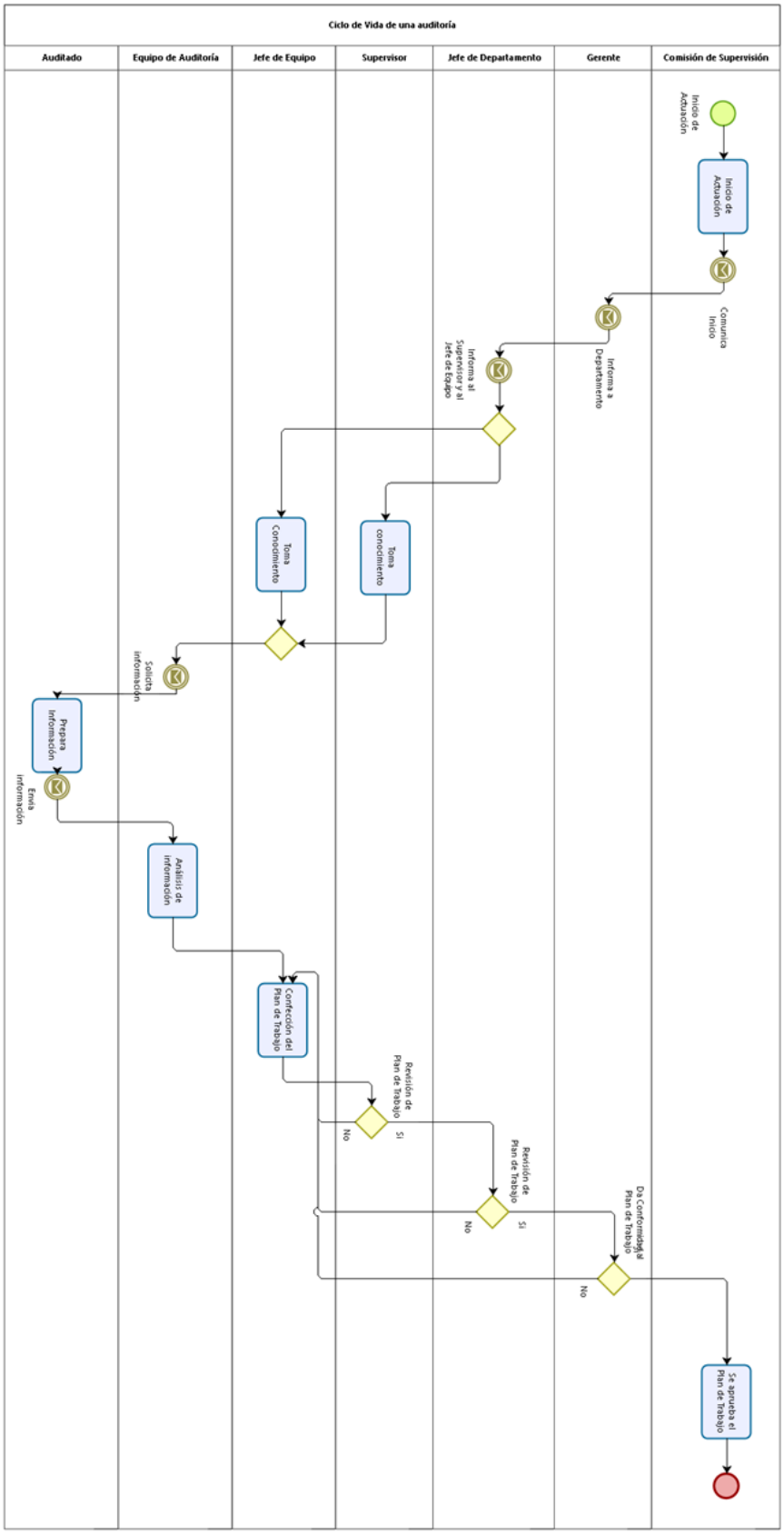
Pasos:

1. La Comisión de Supervisión abre formalmente la actuación, se asigna un número de que la identifica. Se designa al departamento de la AGN que lo llevará a cabo, quiénes serán el supervisor, el jefe de equipo, el equipo actuante y una estimación de tiempos. Se informa a la gerencia correspondiente.
2. Se comunica al departamento correspondiente.
3. Se inician las tareas solicitando datos sobre la estructura de organizacional del auditado e información sobre las principales aplicaciones utilizadas a nivel corporativo.
4. Se recibe la información solicitada.

5. Se analiza la información recibida, se piden reuniones y entrevistas con personal del auditado a fin de aclarar las dudas surgidas de la información recibida.
6. Se confecciona un documento llamado Plan de Trabajo, que consta de una introducción, la materialidad del tema en estudio, el análisis de riesgo, entre otros puntos. Se confecciona una Matriz de Planificación. Se eleva al supervisor.
7. Se revisa el Plan de Trabajo y se lo eleva al Jefe de Departamento.
8. Se revisa y presta conformidad al Plan de Trabajo.
9. Se presta conformidad y se eleva a la Comisión de Supervisión.
10. Se aprueba el Plan de Trabajo.

Diagrama BPM

Ilustración 8 - Diagrama de Planificación de una Auditoría



Fuente: Elaboración propia

Proceso: Ejecución de una auditoría

Roles: Jefe de Equipo

Equipo de Auditoría

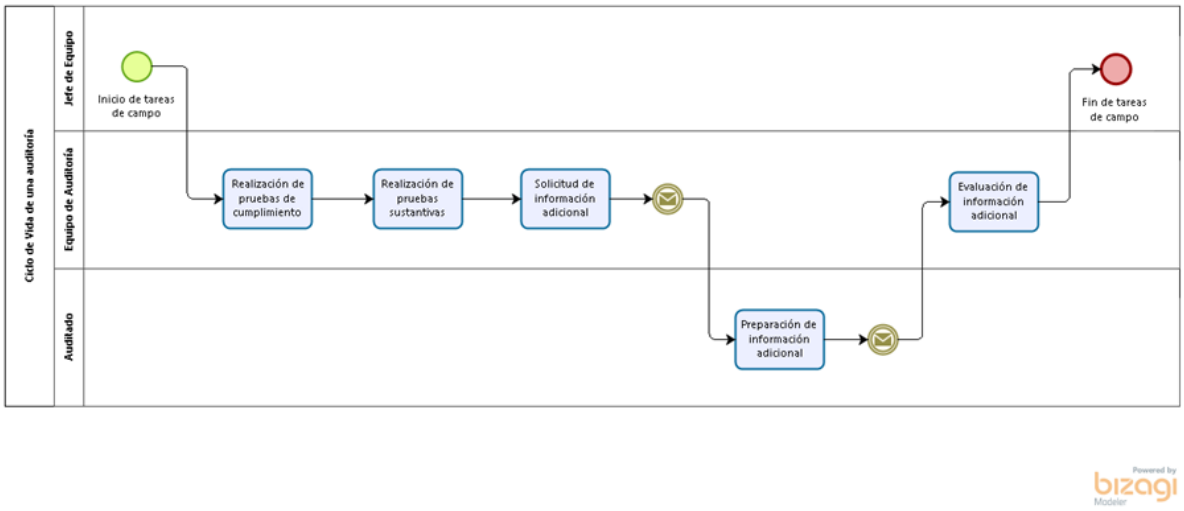
Auditado

Pasos

1. Inicio de tareas de campo.
2. Realización de pruebas de cumplimiento.
3. Realización de pruebas sustantivas.
4. Solicitud de información adicional.
5. Entrega de la información adicional.
6. Evaluación de información adicional
7. Cierre de tareas de campo.

Diagrama BPM

Ilustración 9 - Diagrama de Ejecución de una Auditoría



Fuente: Elaboración propia

Proceso: Informe de una Auditoría.

Roles:

Colegio de Auditores Generales

Comisión de Supervisión.

Gerente.

Jefe de Departamento.

Supervisor

Jefe de Equipo

Equipo de Auditoría

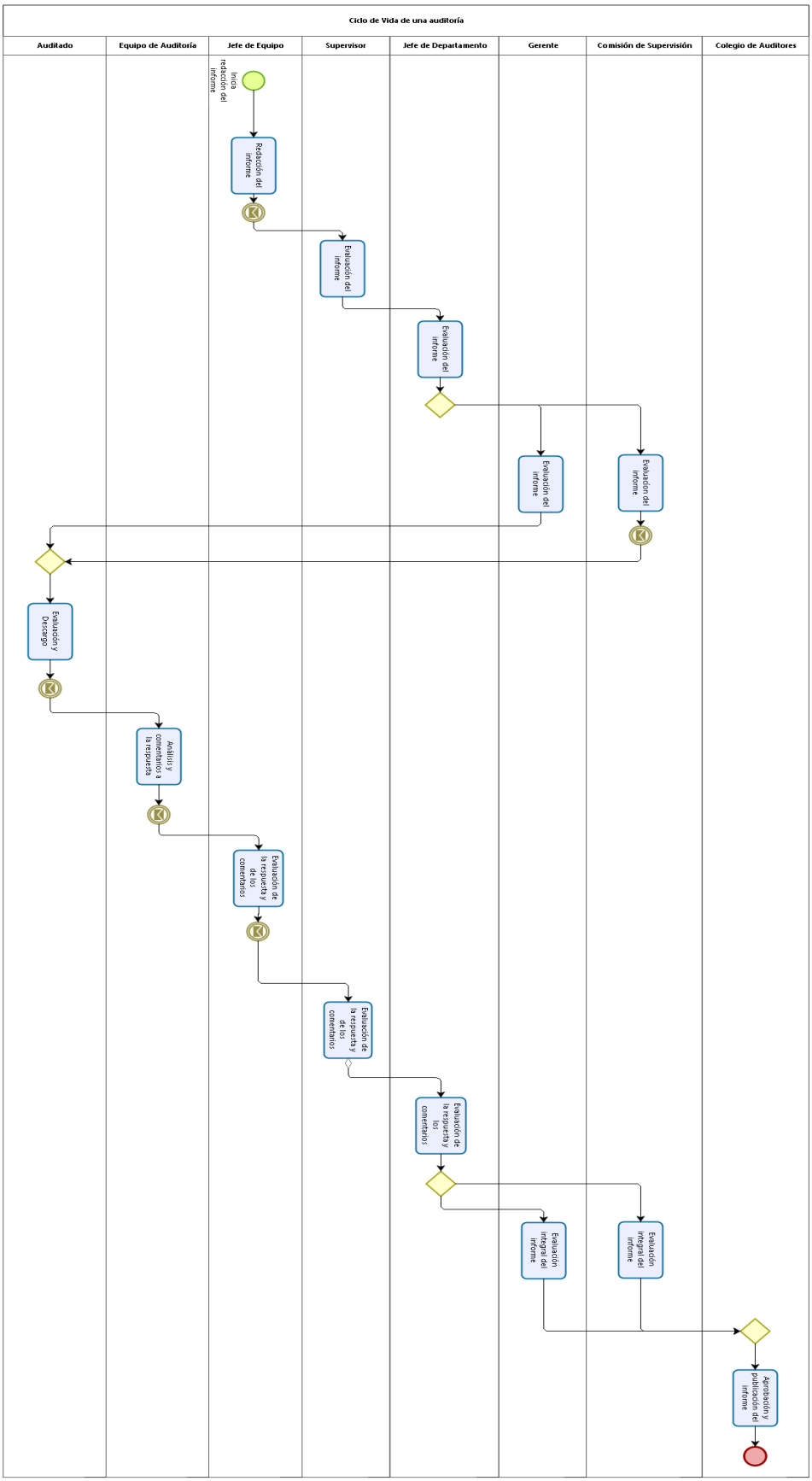
Auditado.

Pasos

1. Se redacta el borrador del Informe de Auditoría.
2. Se hace la primera evaluación del borrador del Informe.
3. Es evaluada para su envío al auditado para que realice su descargo.
4. Evaluación y descargo.
5. Análisis de la respuesta, comentarios a la misma.
6. Primera evaluación de la respuesta.
7. Evaluación del Informe en su conjunto.
8. Aprobación y publicación del Informe.

Diagrama BPM

Ilustración 10 - Diagrama de Informe de una Auditoría



Fuente: Elaboración propia

10. Diagnóstico

10.1 Consideraciones generales

Del relevamiento surge que la AGN no distingue en forma particular a las auditorías de TIC, sino que las considera como un caso particular de las auditorías de gestión. Esta visión no permite tener en cuenta la especificidad propia que las auditorías vinculadas con las tecnologías de información.

10.2 Debilidades encontradas

10.2.1 En la etapa de planificación

Proceso: Planificación de una auditoría

Problema: falta de metodología estandarizada en la etapa de relevamiento para la determinación del Plan de Trabajo.

Causa: No existe un procedimiento formal para obtener información precisa por parte del auditado. Cada auditoría se planifica de manera *ad hoc*, sin seguir una metodología que permita obtener toda la información necesaria para el diseño del Plan de Trabajo de la auditoría.

10.2.2 En la etapa de ejecución

Proceso: Ejecución de una auditoría

Problema: No existe una definición formalizada de cómo realizar los análisis, las pruebas sustantivas y las pruebas de complimiento que sirvan de apoyo y documenten los hallazgos realizados. Estos hallazgos luego se traducirán en las observaciones que constarán en el informe de la auditoría.

Causa: Los criterios que se utilizan para evaluar las distintas debilidades y amenazas encontradas en la etapa de planificación son disímiles, esto provoca que, ante hallazgos similares, las observaciones que se realicen sean esencialmente distintas. Las normas y los parámetros de contrastación quedan a elección del jefe de equipo de auditoría y su equipo.

11. Propuestas de solución

Del conjunto de las debilidades relevadas en la etapa de diagnóstico se puede extraer como primera conclusión la falta de una política definida por parte de la AGN en lo referido al control de TIC en el SPN. Se observa además una falta de madurez en los procedimientos implementados en el Departamento de Auditoría Informática para la realización de auditorías de TIC.

Para solucionar esta situación se propone la redacción de un manual de normas y procedimientos de control de TIC en el cual se definan las políticas y procedimientos que determinen en forma unívoca cómo deben realizarse los análisis, qué normativa debe utilizarse, cuáles serán las pruebas a realizar y los parámetros de contrastación contra los que se verificaran los resultados obtenidos. El cumplimiento de esta normativa será obligatorio en toda auditoría TIC que realice la AGN.

La redacción de este manual debe estar alineada con la normativa vigente en la AGN, como así también tiene que estar basada en las normas más modernas y aceptadas internacionalmente sobre cada tema. Además, debe contener elementos que permitan solucionar los problemas mencionados en el diagnóstico, para ello, se propone lo descripto en el punto a continuación.

11.1 Propuesta de solución general

Propuesta de solución: Incorporar en un Manual de Normas y Procedimientos para el Control Externo de Tecnologías de la Información y Comunicaciones un mecanismo que permita la obtención de la información necesaria para el primer relevamiento de todos los aspectos vinculados a TIC que guarden relación con el objeto de la auditoría. Esta etapa debe incluir un análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) que permitiría identificar las debilidades y amenazas a las que está expuesto el organismo auditado. Además, se debe realizar un análisis de riesgo cuyo resultado será volcado en una matriz que brinde información sobre cuáles son los riesgos inherentes de los procesos, procedimientos, aplicaciones e instalaciones del organismo auditado.

Estos procedimientos deben estar acompañados por un relevamiento del inventario de los recursos TIC que debe realizarse en forma estandarizada de forma tal que todos los organismos sean evaluados con los mismos criterios. Los recursos que deben evaluarse comprenden en principio a los servidores, dispositivos de almacenamiento, dispositivos de conectividad, equipos de seguridad lógica, las aplicaciones corporativas, descripción de los RR.HH. de las áreas involucradas, entre otros puntos.

Los procesos relevados en el punto anterior con la aplicación de la nueva metodología resultan:

Proceso: Planificación de una Auditoría.

Roles:

Comisión de Supervisión.

Gerente.

Jefe de Departamento.

Supervisor

Jefe de Equipo

Equipo de Auditoría

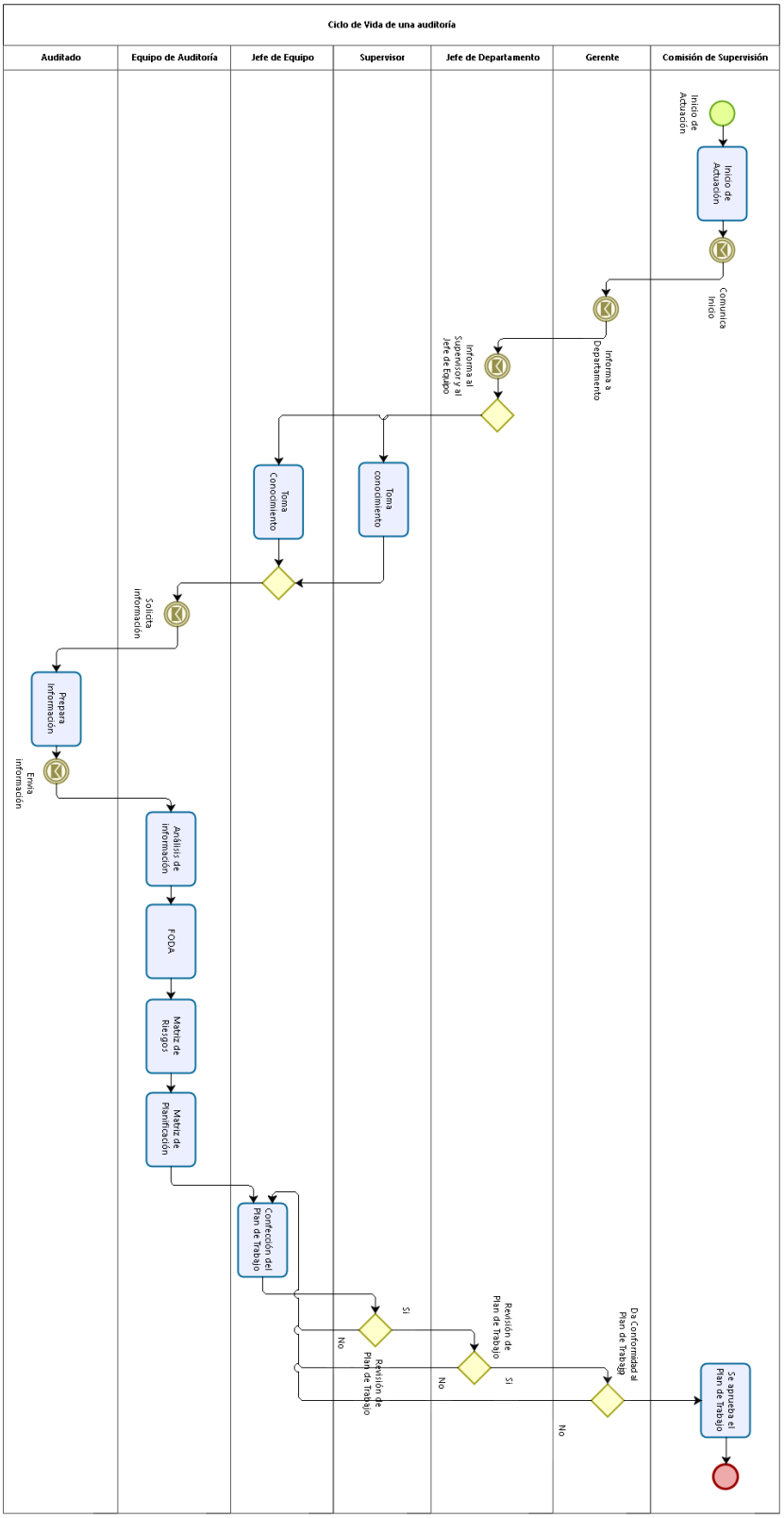
Auditado.

Pasos:

1. Se abre formalmente la actuación, se asigna un número de que la identifica. Se designa al departamento de la AGN que lo llevará a cabo, quiénes serán el supervisor, el jefe de equipo, el equipo actuante y una estimación de tiempos. Se informa a la gerencia correspondiente.
2. Se comunica al departamento correspondiente.
3. Se solicita al ente auditado un inventario de recursos informáticos
4. Se recibe la información solicitada.
5. Se analiza la información recibida, se piden reuniones y entrevistas con personal del auditado con el fin de aclarar las dudas surgidas de la información recibida.
6. Se realiza un análisis FODA
7. Se confecciona una Matriz de Riesgo
8. Se confecciona una Matriz de Planificación
9. Se confecciona un documento llamado Plan de Trabajo, que consta de una introducción, la materialidad del tema en estudio, el análisis de riesgo, entre otros puntos. Se adjunta la Matriz de Planificación. Se eleva al supervisor.
10. Se revisa el Plan de Trabajo y se lo eleva al Jefe de Departamento.
11. El Jefe de Departamento lo revisa y presta conformidad al Plan de Trabajo.
12. El Gerente presta conformidad y se eleva a la Comisión de Supervisión.
13. Se aprueba el Plan de Trabajo.

Diagrama BPM

Ilustración 11- Propuesta de Solución para Planificación de Auditoría



Fuente: Elaboración propia

Proceso: Ejecución de una auditoría

Propuesta de solución: Para minimizar las deficiencias expuestas en el diagnóstico se propone la especificación de procedimientos generales para una auditoría de TIC y específicos para cada uno de los temas analizados. Éstos deben cubrir todos los aspectos relacionados al manejo de las TIC en una organización, de los cuales podemos mencionar:

- Situación del área de TIC respecto del resto de la organización.
- Planificación estratégica del organismo y del área de TIC
- Desarrollo de aplicaciones.
- Aseguramiento de calidad.
- Seguridad informática.
- Continuidad de servicios.
- Relaciones con proveedores.
- Administración de datos.
- Administración de operaciones.
- Administración de instalaciones.

Cada uno de estos puntos será desarrollado como apéndice separado con el fin de poder introducir las actualizaciones necesarias en la medida que los avances de la tecnología así lo requieran.

Todos los procedimientos de control desarrollados deberán estar fundamentados en normas internacionalmente reconocidas, como las expresadas en el punto 7.2 de este trabajo, o en aquellas que se consideren adecuadas para su aplicación, siempre teniendo en cuenta que deben estar avaladas por organizaciones aceptadas por el mercado.

Proceso: Ejecución de una auditoría

Roles: Jefe de Equipo
Equipo de Auditoría
Auditado

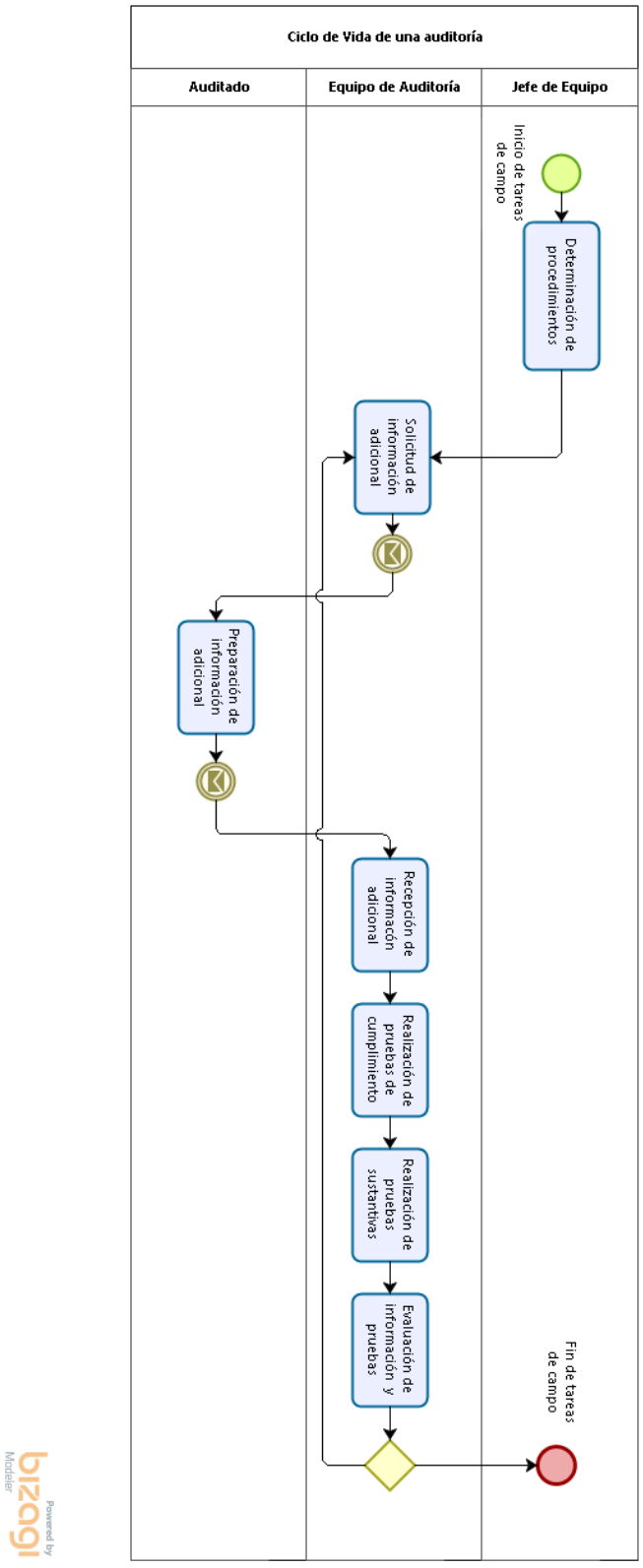
Pasos

1. Inicio de tareas de campo.
2. Determinación de los procedimientos a realizar tomando como base los descritos en el Manual, y los objetivos planteados en el Plan de Auditoría.
3. Solicitud de información adicional.
4. Recepción de la información adicional.

5. Realización de pruebas de cumplimiento.
6. Realización de pruebas sustantivas.
7. Análisis de la información recibida y de las pruebas realizadas
8. Verificación de que la información recibida y las pruebas realizadas sean suficientes.
9. Cierre de tareas de campo.

Diagrama BPM

Ilustración 12 - Propuesta de Solución para Ejecución de Auditoría



Fuente: Elaboración propia

Proceso: Informe de una Auditoría.

En esta etapa, con el fin de mejorar la calidad del producto final del proceso de auditoría, es decir, el informe de auditoría, en el procedimiento de elaboración se incluirán dos etapas más. En una se verificará que se haya cumplido el objetivo propuesto de la auditoría, y en la otra que la evidencia que sustenta los hallazgos sea completa y pertinente.

Proceso: Informe de una Auditoría.

Roles:

Colegio de Auditores Generales

Comisión de Supervisión.

Gerente.

Jefe de Departamento.

Supervisor

Jefe de Equipo

Equipo de Auditoría

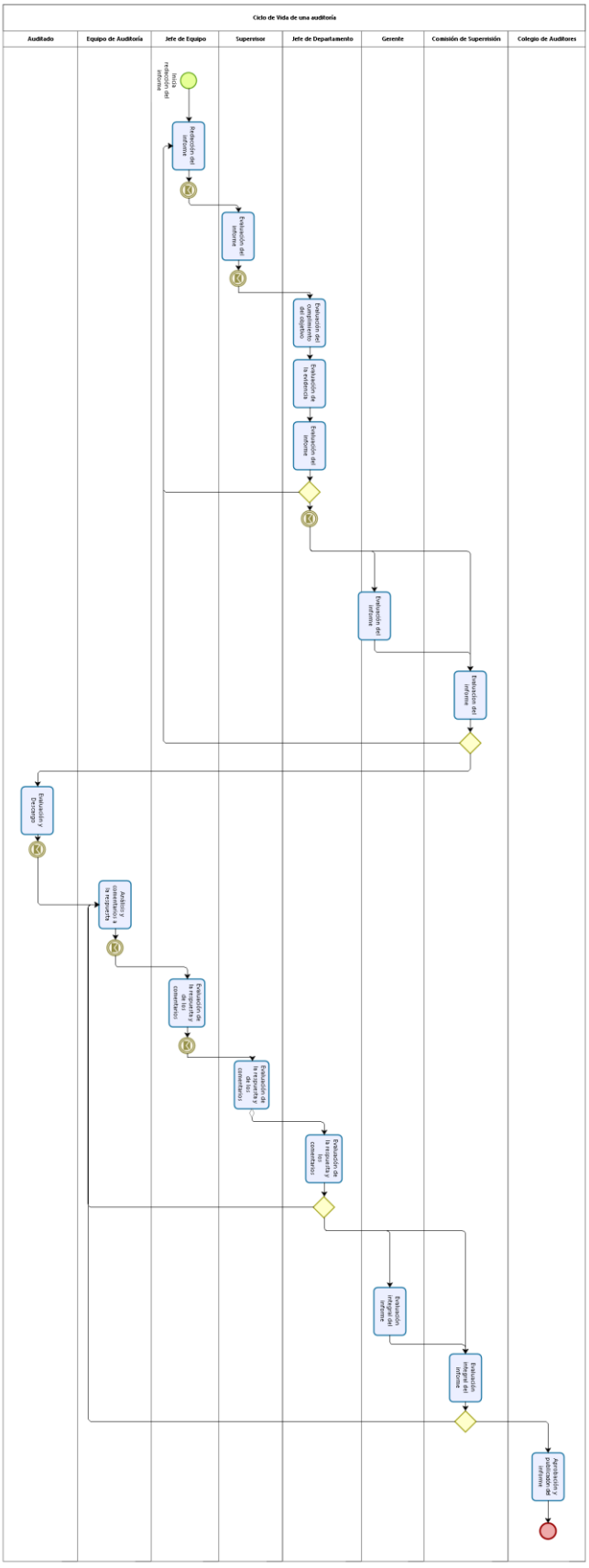
Auditado.

Pasos

1. Se redacta el borrador del Informe de Auditoría.
2. Se verifica que se haya cumplido el objetivo propuesto de la auditoría.
3. Se evalúa que los hallazgos de auditoría estén correctamente fundamentados.
4. Se hace la primera evaluación del borrador del Informe.
5. Es evaluada para su envío al auditado para que realice su descargo.
6. Evaluación y descargo por parte del auditado.
7. Análisis de la respuesta, comentarios a la misma.
8. Primera evaluación de la respuesta.
9. Evaluación del Informe en su conjunto.
10. Aprobación y publicación del Informe.

Diagrama BPM

Ilustración 13 - Propuesta de Solución para Informe de Auditoría



Fuente: Elaboración propia

11.2 Listado de requerimientos funcionales

Como puede observarse el trabajo consiste en el desarrollo de normas y procedimientos para auditorías de TIC. A pesar de no utilizarse la definición de requerimientos funcionales, no funcionales y candidatos en estos casos, se puede establecer una analogía con el desarrollo de un sistema. De esta forma teniendo en cuenta lo expuesto en los puntos anteriores los requerimientos funcionales que debe cubrir este trabajo son:

En el proceso de planificación:

- Desarrollar un modelo de encuesta que permita conocer cuáles son los activos de TIC que dispone el organismo auditado. Este relevamiento debe incluir todas las características técnicas relevantes de cada tipo de dispositivo o servicio, tales como:
    - Servidores
    - Dispositivos de conectividad
    - Dispositivos de seguridad
    - Dispositivos de almacenamiento
    - Enlaces de comunicaciones
    - Dispositivos de soporte (UPS, generadores)
    - Servicios de mantenimiento
    - Dispositivos de ofimática
    - Aplicaciones corporativas
    - RR.HH.
- Formalizar un análisis FODA que permita determinar las amenazas y debilidades del organismo auditado
- Formalizar un análisis de riesgo a partir del FODA que permita determinar cuáles serán los objetivos de la auditoría a realizar.

En la etapa de ejecución: desarrollar un manual de procedimientos de auditoría que abarque los principales escenarios que puedan plantearse. El mismo debe tener completamente definidas las pruebas sustantivas y de cumplimiento a realizarse.

11.3 Listado de requerimientos no funcionales

Los requerimientos no funcionales que se plantean en la confección del manual son los siguientes:

- Claridad en la redacción.
- Debe tener una descripción completa y detallada de los procedimientos a implementar.
- Deben estar alineados con la normativa aprobada por la AGN para la realización de auditorías.
- Debe cumplir con lo que establecido por las normas y estándares:
  - COBIT 4
  - COBIT 5
  - CMMI
  - ITIL
  - IRAM – ISO – IEC 17799
  - ISO 27001
  - ANSI TIA 942
  - PMBOK
  - Auditorías de valor

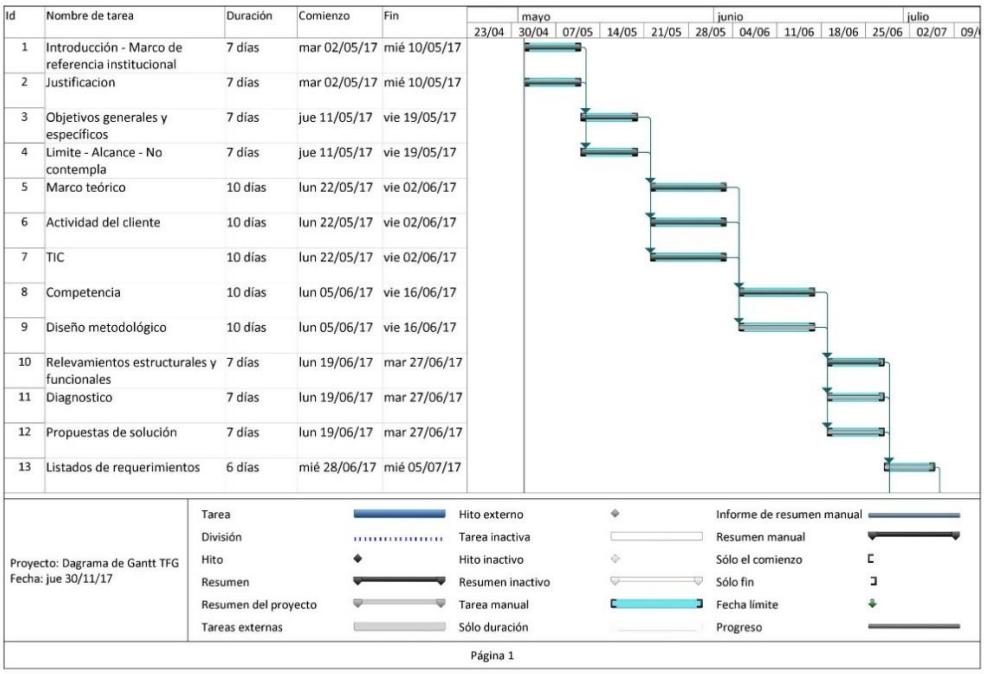
11.4 Listado de requerimientos candidatos

Los requerimientos candidatos para este trabajo son:

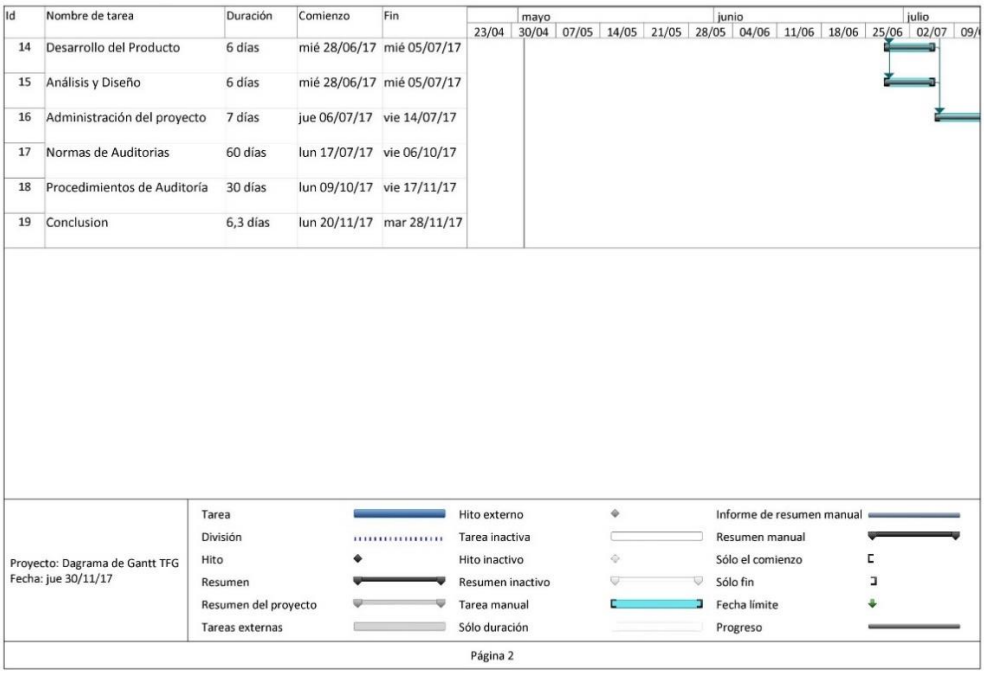
- El desarrollo de un sistema informático que automatice y facilite las tareas de planificación, análisis y pruebas (sustantivas y de cumplimiento) a realizar durante una auditoría de TIC.
- La implementación de un sistema del tipo workflow en el cual se apoye la gestión de la auditoría.
- Un sistema de gestión de comunicaciones que facilite el envío y recepción de solicitudes entre los distintos partícipes del trabajo.
- Un sistema de almacenamiento de información que permita su rápida y eficiente búsqueda mientras se realizan las tareas.

11.5 Diagrama de Gantt

Ilustración 14 - Diagrama de Gantt (!)



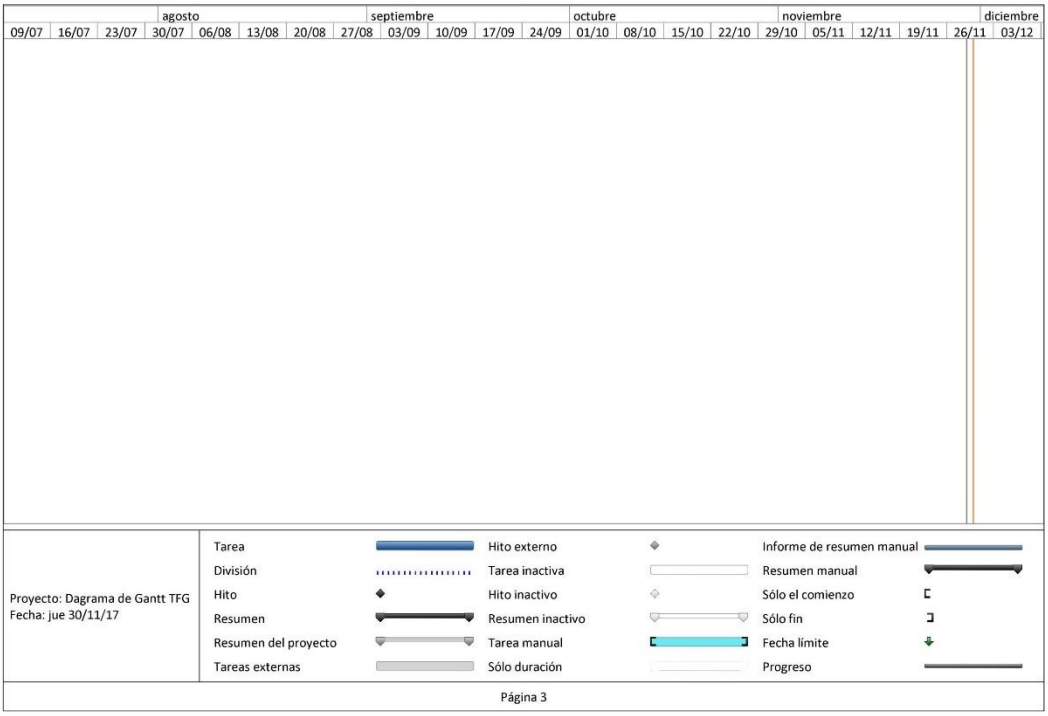
Id	Nombre de tarea	Duración	Comienzo	Fin
1	Introducción - Marco de referencia institucional	7 días	mar 02/05/17	mié 10/05/17
2	Justificacion	7 días	mar 02/05/17	mié 10/05/17
3	Objetivos generales y especificos	7 días	jue 11/05/17	vie 19/05/17
4	Limite - Alcance - No contempla	7 días	jue 11/05/17	vie 19/05/17
5	Marco teórico	10 días	lun 22/05/17	vie 02/06/17
6	Actividad del cliente	10 días	lun 22/05/17	vie 02/06/17
7	TIC	10 días	lun 22/05/17	vie 02/06/17
8	Competencia	10 días	lun 05/06/17	vie 16/06/17
9	Diseño metodológico	10 días	lun 05/06/17	vie 16/06/17
10	Relevamientos estructurales y funcionales	7 días	lun 19/06/17	mar 27/06/17
11	Diagnostico	7 días	lun 19/06/17	mar 27/06/17
12	Propuestas de solución	7 días	lun 19/06/17	mar 27/06/17
13	Listados de requerimientos	6 días	mié 28/06/17	mié 05/07/17

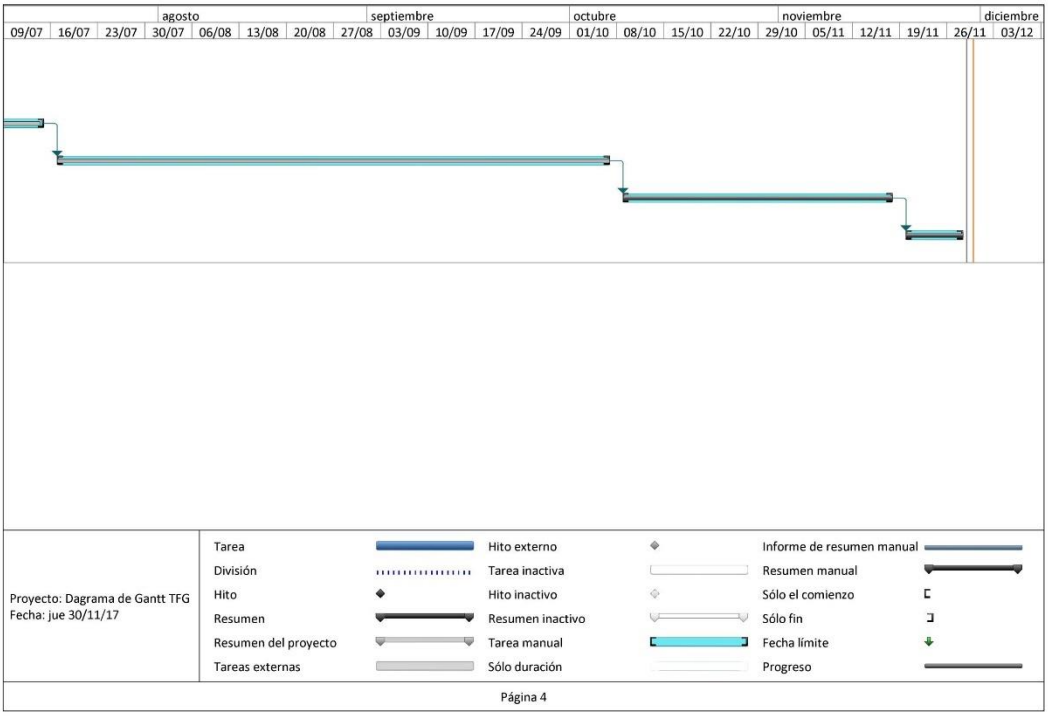


Id	Nombre de tarea	Duración	Comienzo	Fin
14	Desarrollo del Producto	6 días	mié 28/06/17	mié 05/07/17
15	Análisis y Diseño	6 días	mié 28/06/17	mié 05/07/17
16	Administración del proyecto	7 días	jue 06/07/17	vie 14/07/17
17	Normas de Auditorias	60 días	lun 17/07/17	vie 06/10/17
18	Procedimientos de Auditoría	30 días	lun 09/10/17	vie 17/11/17
19	Conclusion	6,3 días	lun 20/11/17	mar 28/11/17

Fuente: Elaboración propia

Ilustración 15 - Diagrama de Gantt (2)





Fuente: Elaboración propia

12. Costos de Recursos Humanos, Hardware y Software

Para este desarrollo todos los recursos utilizados, ya están disponibles en la AGN por lo tanto no se requiere de una inversión adicional para su realización. Sin embargo, se presenta el análisis de costos de desarrollo del mismo.

12.1 Costo de recursos humanos

Se consideró para la realización de esta tarea, un equipo de trabajo compuesto por dos analistas senior, uno de los cuales tendrá la función de Project Leader, y un analista junior. La duración prevista de esta tarea es de 3 meses con dedicación completa, considerando una jornada laboral de 9 horas, y un total mensual de horas de 180 horas.

Resulta entonces:

Tabla 4 - Costo de Recursos Humanos

Cargo	Horas Asignadas [Hs]	Costo por hora´ [$/Hs]	Costo Total [$]
Analista Senior – Project Leader	540	400	216000
Analista Senior	540	340	183000
Analista Junior	540	220	118800

Fuente: Elaboración propia

12.2 Costo del hardware.

Para la elección del hardware, se tomó como referencia la definición de PC de escritorio de la ETAP PC-002-00 v.22 de la Oficina Nacional de Tecnologías de la Información, cuyas características son:

- Arquitectura X86 con soporte USB 3.0 (Universal Serial Bus versión 3.0).
- Setup residente en ROM con password de booteo y setup.
- Capacidad de booteo remoto a través de la conexión LAN.
- Reloj en tiempo real con batería y alarma audible.
- Deberán indicarse otros controles adicionales que posea.
- Procesador no inferior a Pentium (Intel) o A4 (AMD) cuyo lanzamiento al mercado no supere los 12 meses.

- RAM: 4GB (DDR3)
- HDD: 500GB
- Monitor Plano de 19”.
- Teclado y mouse.

Resulta entonces:

Tabla 5 - Costo de Equipamiento

Equipo	Costo Unitario [$/u]	Cantidad [u]	Costo Total [$]
PC de escritorio	15000	3	45000

Fuente: Elaboración propia

Se considera que los equipos vienen equipados con SO Windows y MS Office instalados de fábrica.

12.3 Beneficios esperados

Los cambios propuestos en los procedimientos de auditoría y la estandarización establecida a partir del uso del Manual de Normas y Procedimientos de Control Externo de TIC presenta dos beneficios claves.

El primero si bien es complejo de medir, es quizás el más importante, considerando la relevancia que tienen para la opinión pública es la mejora en la calidad de los informes. Esta nueva metodología sumada al uso de los manuales permitirá la obtención de trabajos más consistentes, con criterios uniformes para los análisis independientemente del organismo bajo estudio.

El segundo beneficio esperado, que sí es posible de estimar, es la disminución de la cantidad de horas hombre utilizadas para la realización de una auditoría.

Como media, se puede considerar que un equipo de auditoría está compuesto por un jefe de equipo, dos analistas senior, dos analistas junior, todos con dedicación full time y un abogado con dedicación part-time. En promedio un equipo de auditoría utiliza 720 horas por empleado con dedicación full-time y la mitad para el abogado para un proyecto estándar.

Resulta entonces:

Tabla 6 - Costo estimado de recursos humanos de un equipo de auditoría – situación actual

Cargo	Horas Asignadas [Hs]	Costo por hora´ [$/Hs]	Costo Total [$]
Jefe de Equipo	720	400	288000
Analista Senior	1440	340	489600
Analista Junior	1440	220	316800
Abogado	360	340	107440
Total			1201840

Fuente: Elaboración propia

Puede considerarse que, con la aplicación de los cambios propuestos los tiempos previstos para los trabajos disminuyen un 20%, resulta así:

Tabla 7 - Costo estimado de recursos humanos de un equipo de auditoría - situación propuesta

Cargo	Horas Asignadas [Hs]	Costo por hora´ [$/Hs]	Costo Total [$]
Jefe de Equipo	576	400	230400
Analista Senior	1152	340	391680
Analista Junior	1152	220	391680
Abogado	288	340	97920
Total			1111680

Fuente: Elaboración propia

De la comparación entre los totales que muestran las dos últimas tablas se observa que puede obtenerse un ahorro del 7.5%.

Si se calcula el Retorno de la Inversión (ROI) del proyecto como **ROI =** cambio en el costo de operaciones / costes de proyecto, resulta:

$$\boldsymbol{ROI = \frac{Cambio\ en\ el\ costo\ deoperaciones}{costo\ del\ Proyecto} = \frac{1201840-1111680}{562800} = 0,16}$$

$$ROI = 16\%$$

Este parámetro indica qué tan beneficioso es encarar el proyecto.

13. Conclusiones

Todo trabajo de auditoría debe ser encarado con un alto grado de estandarización para que el producto de esta tarea resulte confiable, consistente, sin que dependa de las opiniones subjetivas del equipo de auditoría.

Este trabajo se basa en la necesidad detectada en la Auditoría General de la Nación de disponer de un cuerpo normativo detallado para la ejecución de auditorías de TIC.

En la actualidad, el Departamento de Auditoría Informática responsable de este tipo de trabajos utiliza las Normas de Control Externo de Gestión. Si bien este documento pone énfasis en los conceptos de economía, eficiencia, eficacia, y equidad mencionados y definidos en las mejores prácticas de administración de proyectos, no toma en cuenta los conceptos de integridad, confidencialidad y disponibilidad que son claves para el control de las TIC.

Es en este contexto que se desarrolló el trabajo presentado en el Apéndice I, "Manual de Normas y Procedimientos de Control de Tecnología de Información y Comunicaciones. El mismo tuvo en cuenta por un lado el relevamiento de los actuales procedimientos utilizados por el Departamento de Auditoría Informática, y por otro una revisión de las actuales normativas sobre esta materia.

Se encontró dentro de este estudio que las tareas se realizan sin una adecuada planificación, y sin procedimientos estandarizados que aseguren informes de una calidad uniforme. Los resultados de los trabajos de auditoría no dependen de procedimientos formalmente definidos sino de la experiencia y capacidad de los equipos actuantes.

Con respecto al denominado *"ciclo de vida de la auditoría"*, se desarrolló un procedimiento ordenado y preciso que cubre cada una de sus etapas. Además, se estandarizaron las herramientas a utilizar, tanto en la etapa de relevamiento y planificación como de ejecución.

En la evaluación de la normativa existente, se consideraron como más relevantes COBIT en sus versiones 4.1 y 5, CMMI, ITIL, IRAM-ISO-IEC 17799, ISO 27001, ANSI TIA 942, ICREA, PMBOK y Auditorías de Valor. Se encontró que si bien todas estas normas cubren todos los aspectos relacionados con las TIC muchas de ellas se superponen o presentan divergencias en la forma de aplicarlas. Debe tenerse en cuenta también que en general son de alto nivel, sin dar precisiones sobre como deben implementarse las mismas. Por este motivo se seleccionaron los aspectos normativos que se consideraron

necesarios para la realización de auditorías gubernamentales de TIC, y a partir de ellos se definió un conjunto de procedimientos sustantivos que permitan evaluar la gestión de la información en los organismos a ser auditados.

A partir de los antecedentes arriba expuestos se desarrolló este trabajo. El mismo comienza con una breve introducción que describe los principios básicos de control externo gubernamental y el control de las TIC en ámbitos estatales.

El punto siguiente trata sobre las características y condiciones que debe cumplir el auditor externo gubernamental sobre todo en aspectos tales como la competencia profesional, independencia y confidencialidad.

A continuación de describe el ciclo de vida de una auditoría, donde se definen los posibles objetos de una auditoría, y las distintas etapas que componen el proceso de la misma. En cada una de estas etapas se describen las tareas a realizar y las herramientas a utilizar.

Por último, en un Apéndice del mismo, se detallan procedimientos sustantivos a realizar en la ejecución de la auditoría que permitan emitir una opinión confiable acerca del objeto de auditoría.

Con respecto a la implementación de este trabajo, el mismo será presentado oportunamente a las autoridades del organismo para su evaluación y eventual aprobación formal. Igualmente, dentro de las atribuciones del Jefe de Equipo está previsto su uso a modo de prueba para los proyectos que se inicien a partir de Febrero de 2018.

Bibliografía

Asamblea Constituyente. (1994). *Consitución de la Nación Argentina*. Argentina.

Auditoría General de la Nación. (2001). Resolución N° 244/01 - AGN. *Estructura Organizativa*. Argentina.

Auditoría General de la Nación. (2004). Resolución N° 67/04 - AGN. *Estructura Organizativa*. Argentina.

Auditoría General de la Nación. (2008). Resolución Nº 01/08 - AGN. *Estructura Organizativa*. Argentina.

Auditoría General de la Nación. (2015). Resolución 26/2015 AGN. *Normas de Control Externo Gubernamental*. Argentina.

Auditoría General de la Nación. (2016). Resolución N° 186/16 - AGN . *Normas de Control Externo de la Gestión Gubernamental*. Argentina.

Auditoría General de la Nación. (22 de mayo de 2017). Obtenido de http://www.agn.gov.ar/mision

Auditoría General de la Nación. (22 de mayo de 2017). Obtenido de http://www.agn.gov.ar/files/organigrama_05-05-2017_0.pdf

Honorable Congreso de la República Argentina. (1992). Ley N° 24.156 - Ley de Administración Financiera y de los Sistemas de Control del Sector Público Nacional. Argentina: Boletín Oficial.

Information Systems Audit and Control Association. (2012). *COBIT 5*. Rolling Meadows,, IL, EE UU.

Instituto Argentino de Normalización y Certificación. (2005). *IRAM - ISO/IEC 17799 - Information Technology. Code of practice for information security management.* Argentina.

Instituto Argentino de Normalización y Certificación. (2007). *IRAM - ISO/IEC 27001 Sistemas de gestión de la seguridad de la información (SGSI).* Argentina.

Instituto de Auditores Internos de Argentina. (24 de septiembre de 2017). Obtenido de https://iaia.org.ar/auditor-interno/definicion-auditoría-interna

International Computer Room Experts Association. (20 de mayo de 2017). *Norma ICREA std 131-2015*. Obtenido de http://www.icrea-international.org/nuevoPortal/index.asp

International Organisation of Supreme Audit Institutions. (2013). *Manual de la IDI y WGITA sobre auditorías de TI para las entidades fiscalizadoras superioResolución N°* Pekin, China.

IT Governance Institute. (2007). *CobiT 4.1.* Rolling Meadows,, Il, EE UU: IT Governance Institute.

Natale, A. (1995). *Comentarios sobre la Constitución La Reforma de 1994.* Buenos Aires, Argentina: Ed. Depalma.

Project Management Institute, Inc. (2013). *PMBOK'S Guide.* Newtown Square, PA, EE UU: Project Management Institute, Inc.

Real Academía Española. (18 de septiembre de 2017). *Diccionario de la Lengua Española*. Obtenido de http://dle.rae.es/?id=4NVvRTc

Software Engineering Institute. (2010). *Software Engineering Process Management Program.* Hanscom AFB, MA, EE UU: Carnegie Mellon University.

Tribunal de Cuentas Europeo. (24 de septiembre de 2017). *Manual de Auditoría de Gestión 2015.* Obtenido de http://www.eca.europa.eu/Lists/ECADocuments/PERF_AUDIT_MANUAL/PERF_AUDIT_MANUAL_ES.PDF

Apéndice I

Manual de Normas y Procedimientos de Control de Tecnologías de Información y Comunicaciones

I – Introducción

Este Manual de Normas de Control de Tecnologías de Información y Comunicaciones tiene como objetivo servir de herramienta de estandarización de procedimientos y métodos que serán aplicados por la Auditoría General de la Nación en todos los trabajos que se realicen sobre la materia.

El uso de herramientas informatizadas es relativamente nuevo para las personas y organizaciones. Sus primeros usos prácticos comienzan en la década de 1940, avanzando en forma rápida y sostenida en las décadas de los años 60 y 70, con la aparición de los microprocesadores de estado sólido, y de lenguajes de programación más potentes y versátiles. En la última década del siglo pasado y los años que transcurrieron en este siglo su avance fue explosivo, por un lado, por la aparición de la WEB y por otro por el avance en las distintas tecnologías en materia de comunicaciones. Si bien estas dos ramas de la tecnología hasta finales del siglo pasado se desarrollaron en forma independiente, su confluencia transformó totalmente la cultura en todos sus aspectos.

Como es lógico, este brutal cambio de paradigmas tuvo un fuerte impacto en todas las organizaciones tanto privadas como gubernamentales. Hoy es impensado que un ente administrativo de la rama que sea se maneje sin estar apoyado en una estructura informática sólida y confiable para la ejecución de sus tareas.

Estos cambios tuvieron también su correlación en el campo de la auditoría. Inicialmente los controles que se realizaban a los sistemas informáticos eran controles físicos a los equipos y sobre el desarrollo de los programas. Con el avance de la tecnología, se abandona el concepto de Auditoría Informática y se introduce el concepto de Auditoría de Sistemas de Información. Más tarde con la aparición de la WEB y los avances de las comunicaciones, entre otros adelantos, se transforman en Auditorías de Tecnologías de la Información y Comunicaciones por estar estos conceptos íntimamente relacionados.

Este nuevo campo, por sus características particulares, toma en cuenta conceptos de otras ramas del control, como las auditorías de gestión o las auditorías de cumplimiento, pero dada la especificidad y amplitud de los temas que abarca debe considerársela como un tipo independiente de auditoría.

Teniendo en cuenta entonces, el estado actual de los avances tecnológicos y organizaciones de las empresas u organismos se desarrolló este manual como guía de para las tareas de control externo de sistemas de información.

I – A – Objetivos de los Trabajos de Control Externo Gubernamental.

En cumplimiento del artículo 85 de la Constitución Nacional, la función de realizar el control externo del Sector Público Nacional verificando el desempeño y la situación general de la administración pública en sus aspectos patrimoniales, económicos, financieros y operativos es una atribución del Poder Legislativo.

La Auditoría General de la Nación, de acuerdo con la Ley 24.156 de Administración Financiera, es el órgano rector de control externo y tiene competencia para el dictado de las normas técnicas que rigen en la materia. Por este motivo goza de autonomía funcional con el fin de asegurar su independencia.

El control gubernamental se aplica por un lado sobre la gestión, que es responsabilidad de los funcionarios designados en el Poder Ejecutivo Nacional y por otro, sobre los organismos que utilicen fondos públicos para la prestación de servicios a los ciudadanos.

El control busca generar las condiciones adecuadas para que los organismos del Sector Público Nacional y los funcionarios responsables de los mismos realicen las tareas asignadas de manera eficaz, eficiente, cumpliendo con las leyes que los regulan.

Las evaluaciones que realiza la Auditoría General de la Nación quedan expresadas en informes escritos, en los cuales se detallan el objetivo y el alcance de la auditoría, los métodos utilizados, la situación encontrada proponiéndose además las mejoras necesarias para solucionar las deficiencias encontradas con el fin de que los organismos puedan brindar un nivel de servicio adecuado a la ciudadanía.

De acuerdo con la Resolución N°26/2015 de la AGN, los trabajos de control externo:

- Proporcionan información objetiva, independiente y confiable.
- Proporcionan conclusiones y opiniones basadas en evidencia suficiente y apropiada.
- Promueven la mejora en la rendición de cuentas gubernamental, brindando credibilidad y transparencia.

- Fortalecen la eficacia de los entes rectores y aquellos responsables de la administración de actividades con fondos públicos.
- Crean incentivos para el cambio a través de análisis completos y recomendaciones de mejoras bien fundamentadas.

I – B – Principios Básicos del Control Externo de las TIC en el Ámbito Gubernamental

Como ya fuera expresado anteriormente las Tecnologías de la Información y Comunicaciones son de uso obligado en cualquier organización. El ámbito gubernamental no escapa a esta situación y su control es fundamental para el éxito en su tarea de administrar bienes y recursos o brindar servicios al ciudadano. No existe hoy área gubernamental que no necesite del uso intensivo de soportes informáticos para el tratamiento de sus datos, y de un esquema sólido de comunicaciones para que la información circule eficientemente dentro de la organización.

La Administración Pública Nacional es, sin dudas, quien administra, almacena y difunde la mayor cantidad de información del país. Organismos como la Administración Federal de Ingresos Públicos (AFIP), la Administración Nacional de la Seguridad Social (ANSES) o el Registro Nacional de las Personas (RENAPER) son ejemplos de manejo de grandes volúmenes de información.

En este sentido debe considerarse a la información gubernamental un recurso valioso porque brinda al ciudadano conocimientos sobre el gobierno, la sociedad y el estado de la gestión pública.

El campo de la auditoría de control externo de las tecnologías de la información y comunicaciones es amplio y abarca

- Las organizaciones y sus estructuras.
- Las inversiones sobre TIC.
- Los procesos de las TIC.
- Los sistemas informáticos.
- Los proyectos sobre TIC.
- La seguridad de la información.
- Las comunicaciones y redes de trasmisión de datos.

Este flujo de información entre el gobierno y el ciudadano debe ser libre y transparente, siendo el mantenimiento de estas condiciones una de las más importantes tareas de cada uno de los organismos, y debe estar limitada únicamente por aquellos temas que la legislación expresamente define como secretos (como por ejemplo los temas vinculados a seguridad tanto interna como externa, entre otros) y por cualquier acción que pueda afectar el derecho del individuo a la privacidad.

Con respecto al párrafo anterior es importante resaltar la importancia que tienen los tres atributos de la seguridad de la información:

- confidencialidad,
- integridad,
- disponibilidad.

Éstos deben ser objeto de cuidadosos análisis en todas las auditorías que se realicen con el fin de asegurar su cumplimento.

Uno de los aspectos más importantes en el uso de las TIC es su rápida evolución, de la mano de los avances tecnológicos cada vez más rápidos, que obligan a cambios permanentes de los paradigmas utilizados para las auditorías. Debe entonces preverse que los recursos físicos y principalmente los humanos se encuentren permanente actualizados con el fin de poder realizar las tareas de auditoría con la calidad requerida.

La Ley 24.156 establece el régimen de rendición de cuentas por la responsabilidad asignada al funcionario público. En este marco los objetivos que se deben cumplir son:

a. Garantizar principios de regularidad financiera, legalidad, economía, eficiencia, y eficacia.
b. Evaluar programas, proyectos y operaciones de las Jurisdicciones y/o Entidades.
c. Sistematizar las actividades de programación, gestión y evaluación
d. Desarrollar sistemas de información oportuna y confiable, útil para la dirección y para evaluar la gestión de los responsables de cada una de las áreas.

Se observa que si bien de estos últimos cuatro puntos, sólo el último menciona textualmente a los sistemas de información. Es indudable que el cumplimiento de los 3 primeros es imposible pensarlos sin el apoyo de una estructura informática que permita gestionar eficaz y eficiente los grandes volúmenes de datos involucrados en estas tareas. Por tal motivo es indispensable disponer de todos los recursos informáticos necesarios, tanto en equipamiento e infraestructura como en RR.HH. para poder realizar las tareas de control necesarias con el fin de cumplir en principio con lo dispuesto por la Ley, pero

también satisfacer lo que espera la ciudadanía del cuidado en el manejo que los recursos que la misma brinda a los funcionarios del estado para el cumplimento de sus funciones.

II – El Auditor de TIC

II – A - Características Generales del Auditor Externo Gubernamental

Tal como lo establecen las Normas de Control Externo Gubernamental de la Auditoría General de la Nación, el auditor gubernamental debe cumplir con los principios éticos que el organismo establece, los que le son aplicables en el ejercicio de la función pública, y los códigos de ética fijados en las normas de ejercicio profesional.

II – B - Características Generales del Auditor Externo Gubernamental de TIC

Las condiciones expuestas a continuación deben ser cumplidas tanto por el personal propio de la AGN que realice auditorías de TIC como por aquellos expertos que sean contratados específicamente para complementar el conocimiento del equipo de auditoría.

II – B – 1 – Competencia Profesional

El auditor gubernamental de TIC deberá tener conocimiento de las organizaciones gubernamentales y programas, de forma tal de entender las leyes, decretos y reglamentaciones que rigen las acciones de los organismos a los que los sistemas informáticos deben dar soporte.

En general, los equipos de auditoría deberán contar con distintos especialistas a fin de cubrir las diversas áreas de las Tecnologías de la Información y Comunicación, entre ellas podemos mencionar:

- Análisis y Diseño.
- Programación
- Testing
- Comunicaciones
- Seguridad Informática.
- Infraestructura

Debe tenerse especialmente en cuenta que el auditor externo gubernamental no cumple funciones de asesoría, su campo es la auditoría y sus recomendaciones deben ser

genéricas siendo el auditado quien decida la forma y el detalle en que dichas recomendaciones serán puestas en práctica.

El auditor gubernamental de TIC deberá poseer la formación técnica y la experiencia profesional adecuadas para realizar las tareas que le sean asignadas. Es indispensable que tenga sólidos conocimientos en los aspectos relacionados con las Tecnologías de Información y Comunicaciones, tales como infraestructura, hardware, software de base, software de aplicaciones, redes de comunicación, bases de datos, entre otros.

Debe ser capaz de diseñar los procedimientos para la realización de las pruebas sustantivas necesarias para un eficaz control de los objetivos asignados.

II – B – 2 – Independencia el Auditor

Con el fin de emitir una opinión objetiva e imparcial, fundamentada únicamente por su conocimiento técnico, sin estar influenciada por factores o intereses externos, es fundamental que el auditor sea independiente y que así sea considerado por el auditado.

Tal como se encuentra definido en las Normas de Control Externo Gubernamental (AGN, 2015) "se considera independencia de criterio a aquel estado que permite proporcionar una opinión que no se vea afectada por influencias que comprometan su criterio profesional, permitiendo que un individuo actúe con integridad y ejerza su objetividad".

Los factores que pueden afectar la independencia de criterio son:

a) Amenazas de interés propio: por la existencia de intereses personales del auditor con relación al ente objeto de la auditoría. Esto incluye a familiares cercanos al auditor o por tener relaciones personales con directores, funcionarios, gerentes o administradores del organismo auditado.
b) Amenazas de seguimiento: cuando una opinión anterior es reevaluada por el mismo auditor gubernamental.
c) Amenazas de intermediación: cuando el auditor promueve una posición, hasta que su objetividad puede verse comprometida.
d) Amenazas de familiaridad: cuando por relaciones de cercanía el auditor se muestre comprensivo con los intereses del auditado.
e) Amenazas de intimidación: cuando el auditor es amenazado en forma real o percibida para emitir una determinada opinión.

f) Amenazas de pertenencia: cuando el auditor haya estado vinculado o participado en operaciones o programas que estén vinculados con el objeto de la auditoría, o hayan formado parte del organismo auditado.
g) Amenaza de conflicto de intereses: se produce cuando exista algun tipo de interés en el auditor, que pueda condicionar o interferir para que el mismo no actúe con la imparcialidad necesaria para el cumplimiento de su tarea.

Ante cualquiera de los casos mencionados, el riesgo de que se produzca la amenaza debe ser eliminado o mitigado. De no ser posible, el auditor deberá excusarse de continuar con el proyecto informando de la situación por escrito a su superior inmediato.

II – B – 3 – Compromiso de Confidencialidad

El auditor gubernamental no debe revelar la información obtenida en las tareas de auditoría a terceros, a menos que la misma sea solicitada por motivos legales o profesionales.

La información que el auditor gubernamental adquiera con motivo de su tarea no debe ser utilizada para obtener beneficios propios o para terceros.

III – Ciclo de una Auditoría

Se entiende como Ciclo de una Auditoría, a todo el proceso que se desarrolla desde la selección de los objetos de auditoría, hasta el seguimiento de las recomendaciones de las auditorías realizadas, en el caso que el mismo sea realizado.

III – A – Selección de los Objetos de Auditoría

III – A – 1 - Universo Auditable

De acuerdo con el artículo. 85 de Constitución Nacional y la Ley N° 24.156, Ley de Administración Financiera, la Auditoría General de la Nación tiene como función principal el control externo del Sector Público Nacional. Por tal motivo pueden ser objeto de auditorías todos los entes u organismos de Administración Pública Nacional, los Fondos Fiduciarios, los organismos descentralizados, las instituciones de la Seguridad Social, las empresas públicas nacionales, sociedades del Estado, entes reguladores de servicios públicos, y los entes privados adjudicatarios de procesos de privatización.

III – A – 2 – Selección de la Materia a Auditar

La AGN debe presentar ante la Comisión Mixta Revisora de Cuentas, su Plan Operativo Anual (POA), en el cual se detallan todos los trabajos que se realizaran durante el próximo ejercicio fiscal.

Para seleccionar los proyectos a incluirse en el POA deberán considerarse los siguientes criterios:

- Significatividad: tiene en cuenta la magnitud de los recursos económicos o la relevancia de la materia para la opinión pública
- Riesgo: tiene en cuenta los riesgos asociados al tema bajo estudio, específicamente, los riesgos inherentes, de control y de detección.
- Auditabilidad: tiene en cuenta la posibilidad técnica de realizar la auditoría.

Los proyectos pueden ser propuestos por el Colegio de Auditores Generales, la Gerencia de la cual depende el Departamento de Auditoría Informática, o el mismo departamento de acuerdo a estudios que haya realizado.

III – B – Proceso de Auditoría

III – B – 1 Planificación

En esta etapa se determina el objetivo y alcance de la auditoría. Esto permite estimar los recursos necesarios y los plazos para su ejecución. Es una etapa clave del ciclo de vida de la auditoría, que comienza con la apertura de la misma y finaliza con la aprobación del plan de trabajo.

La planificación de una auditoría es un proceso dinámico que se realiza al comienzo de la auditoría, pero que puede ser modificado durante su ejecución, de acuerdo a la información recibida y los hallazgos que se vayan produciendo.

Para una correcta planificación de una auditoría deben estar definidos su alcance y el período auditado, que son los elementos que definirán los procesos y sectores que se analizarán.

En esta etapa, el equipo de auditoría debe entender lo más completamente posible las funciones del organismo auditado, su estructura, la materia en cuestión, conocer cuáles son las áreas involucradas y quiénes son los principales interesados.

III – B – 1 – a - Apertura y Solicitud Inicial de Información

El Departamento Auditoría Informática solicitará el inicio de auditoría mediante una nota a la Gerencia de Planificación para que la misma sea elevada a la Comisión de Supervisión y ésta disponga el comienzo de las tareas. La solicitud deberá incluir el objeto de la auditoría, el detalle del equipo actuante y los plazos de inicio y fin (este último, tentativo).

La Comisión de Supervisión notificará del inicio de la auditoría al organismo a ser auditado mediante una nota que será acompañada por una solicitud inicial de información. Para ello se enviarán planillas en hojas de cálculo en un CD que solicitarán el detalle de los recursos informáticos disponibles, tanto en equipamiento, infraestructura, como en recursos informáticos (Ver ANEXO I).

III – B – 1 – b - Relevamiento Inicial

- Legajo permanente del organismo en la AGN.
- Página WEB institucional.
- Búsqueda por Internet de información relacionada con el organismo o el tema bajo estudio.
- Entrevistas con personal responsable del organismo.
- Entrevistas con responsables de entes u organismos (por ejemplo, otros organismos estatales, ONGs), vinculados al que se encuentra bajo estudio.
- Informes de auditoría interna.

Toda la información será evaluada por el equipo de auditoría para tener una visión detallada de la organización y del o los procesos que están siendo auditados.

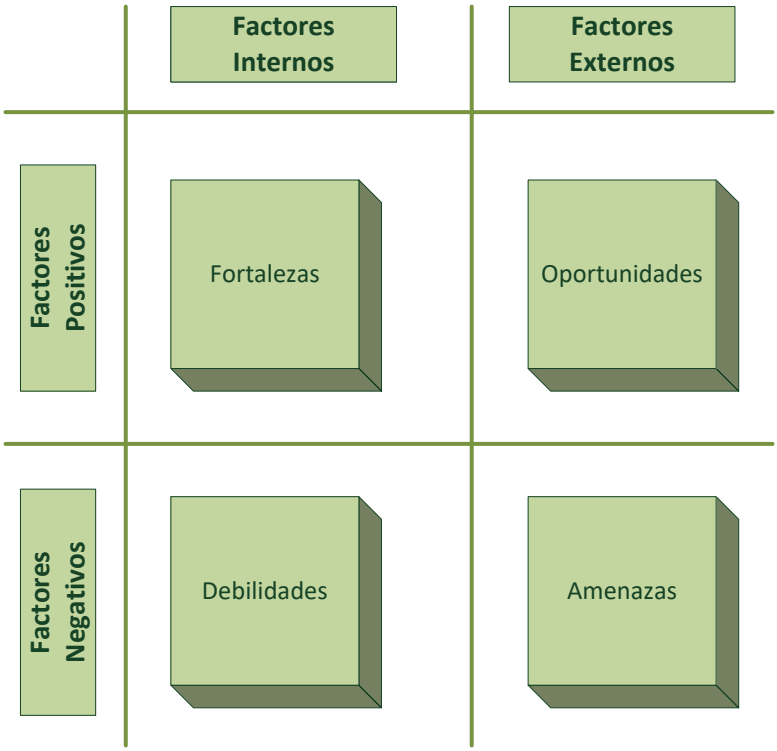
III – B – 1 – c - FODA (Fortalezas, Oportunidades, Debilidades y Amenazas)

Una vez analizada toda la información recibida inicialmente se procederá a realizar un análisis FODA en el cual se detallarán con el mayor grado de precisión posible todas las fortalezas, oportunidades, debilidades y amenazas que tienen tanto la organización en su conjunto, como los procesos a ser evaluados. En este análisis las oportunidades y amenazas representan a las fuerzas del mercado, mientras que las fortalezas y debilidades corresponden a características propias de la organización.

- Oportunidades: representan una ocasión de mejora de la empresa. Son factores positivos que pueden ser explotados.

- Amenazas: pueden poner en peligro la supervivencia de la organización o en menor medida afectar las operaciones de la misma.
- Fortalezas: Son todas aquellas capacidades y recursos con los que cuenta la empresa para explotar oportunidades.
- Debilidades: Son aquellos puntos de los que la empresa carece, o aquellos en los que se puede mejorar.

Ilustración 16 - FODA



Fuente: Elaboración Propia

III – B – 1 – d - Matriz de Riesgo

A partir de la información obtenida y del análisis FODA realizado es posible identificar los riesgos.

Se puede considerar al riesgo como la probabilidad de que un evento afecte negativamente el cumplimiento de los objetivos de un ente o las operaciones del mismo. Por lo tanto, el riesgo de auditoría está vinculado con la estructura del organismo y las personas que trabajan en él.

Los riesgos de auditoría pueden clasificarse en:

- Riesgo inherente.
- Riesgo de control
- Riesgo de detección.

El riesgo inherente representa la posibilidad de que determinadas operaciones tengan errores, independientemente de los sistemas de control en funcionamiento. Este riesgo es propio de la organización y del procedimiento bajo estudio.

El riesgo de control es la posibilidad de que existan errores en las transacciones que no fueron prevenidos o detectados y corregidos por los sistemas de control implementados.

El riesgo de detección es el que se produce cuando los procedimientos sustantivos aplicados por el auditor no detectan un error en una transacción o en un procedimiento.

Las dos primeras categorías se encuentran fuera del control del auditor y son propias de los sistemas y actividades del ente auditado, mientras que la tercera está directamente relacionada con las tareas del auditor.

Para cuantificar los riesgos detectados se los clasifica en 4 grados posibles:

- Riesgo mínimo.
- Riesgo bajo.
- Riesgo medio.
- Riesgo alto.

Debe tenerse en cuenta que la evaluación de riesgos es un proceso subjetivo y depende exclusivamente del criterio, capacidad y experiencia del auditor.

Para reducir el grado de subjetividad del riesgo se buscará medir tres elementos que combinados permiten definir el nivel de riesgo:

- La significatividad del componente.
- La existencia de factores de riesgo.
- La probabilidad de ocurrencia de errores o irregularidades.

Las combinaciones posibles de estos tres elementos permiten evaluar el riesgo de auditoría de acuerdo al cuadro siguiente:

Ilustración 17 - Tabla de Riesgos

Nivel de riesgo	Significación	Factores de riesgo	Probabilidad de ocurrencia
Mínimo	No significativo	No existen	Remota
Bajo	Significativo	Existen algunos de menor importancia	Improbable
Medio	Muy significativo	Existen algunos	Posible
Alto	Muy significativo	Existen varios y son importantes	Probable

Fuente: Elaboración propia

III – B – 1 – e – Plan de Auditoría

Todas las tareas realizadas serán volcadas en un Plan de Auditoría, que es un documento formal preparado por el equipo de auditoría (ANEXO II), y será elevado por el Jefe de Equipo a su superior inmediato para que, siguiendo la cadena de jerárquica, el mismo llegue a la Comisión de Supervisión correspondiente que será quien lo apruebe y ordene la continuidad de las tareas. Este plan debe elevarse antes de cumplir el 50% de la cantidad de horas totales asignadas al proyecto.

Este documento resume el trabajo a realizar y los resultados que se pretenden alcanzar explicando el enfoque y los procedimientos que se utilizarán. Presenta un marco conceptual del tema bajo estudio y un marco normativo e institucional bajo el cual está sujeto el organismo.

También incluye el cronograma de ejecución, los recursos a utilizar, el personal que realizará las tareas con sus funciones y detalla si es necesario la contratación de especialistas externos.

El Plan de Trabajo debe incluir la matriz de riesgos descripta en el punto anterior y una Matriz de Planificación (Anexo III) donde se resumen los procedimientos necesarios que permitan conocer cuáles son los procesos y procedimientos que se aplicarán en la ejecución de la auditoría.

Los principales objetivos que debe cumplir la Matriz de Planificación son:

- Establecer una relación lógica entre los objetivos, la información requerida y los procedimientos que se realizarán en los trabajos de campo.
- Exponer las decisiones de planificación.

- Facilitar la supervisión y control de las tareas realizadas.

III – B – 2 – Ejecución

El objetivo de esta fase está orientado a la obtención de evidencias y la formulación de observaciones con sus respectivas recomendaciones sobre las áreas y procesos auditados utilizando las herramientas y procedimientos aprobados en el Plan de Auditoría.

Debe realizarse conforme a la planificación previamente aprobada por la Comisión de Supervisión.

Las actividades que se realizan en esta etapa son:

- Desarrollo del trabajo de campo con el fin de obtener evidencia: consiste en la recolección de la mejor evidencia posible, que debe ser adecuada en cantidad y calidad.
- Análisis de la información obtenida: consiste en la selección y estudio de la información recolectada que permita responder las preguntas planteadas en la planificación. Una vez terminada esta tarea deben revisarse los análisis de riesgo, materialidad y criterios establecidos en el Plan de Auditoría para evaluar si son necesarios procedimientos adicionales con el objeto de sustentar los hallazgos, conclusiones y recomendaciones.
- Desarrollo de los hallazgos de auditoría.

Las herramientas a utilizar son todas aquellas que permitan la obtención de evidencia suficiente y apropiada para sustentar los hallazgos, resultados y conclusiones del informe. El auditor determinará la naturaleza, los tiempos de ejecución y el alcance de los procedimientos que se realizarán.

Los procedimientos para obtener evidencia pueden ser:

- Inspección: es el examen de registros o documentos internos o externos.
- Observación: ejecución de un procedimiento por parte del auditor o presenciar un proceso o procedimiento aplicados por otras personas.
- Investigación: consiste en solicitar información crítica a personas tanto del área objeto de control, como externas a él. Las respuestas pueden suministrar información relevante que puede apoyar o contrastar otra recibida por el auditor.

- Conformación externa: evidencia de auditoría obtenida mediante una respuesta directa escrita por un tercero y dirigida al auditor.
- Recálculo: consiste en comprobar la exactitud de los cálculos matemáticos incluídos en los documentos o registros.
- Re-ejecución: consiste en la ejecución independiente de procedimientos o de controles que en origen fueron realizados por la entidad.
- Procedimientos analíticos: evaluaciones de información realizadas mediante el estudio de las relaciones que debieran existir entre los datos.
- Recopilación de datos: pueden provenir de cuestionarios, encuestas, entrevistas presenciales referidas a la totalidad de la población controlada o una parte de ella.

Para una auditoría gubernamental de TIC es indispensable evaluar los siguientes aspectos:

- Estructura Organizacional
- Funciones Organizacionales.
- Administración de Proyectos – Gestión de Ciclo de Vida.
- Análisis de la Seguridad de la Información.
- Análisis de la Infraestructura.
- Análisis de Bases de Datos.
- Análisis de Control Interno.

Cada uno de los temas mencionados tiene sus propios procedimientos, los cuales se detallan al final de este documento.

Después de la aplicación de los procedimientos que el auditor considere pertinentes para la obtención de la evidencia deberá verificar que la misma sea válida, relevante, confiable y suficiente para sustentar conclusiones razonables.

La evidencia obtenida puede ser:

- Física: mediante la inspección u observación directa de bienes, procesos o procedimientos realizados por terceros.
- Documental: proviene del examen de registros, documentos, contratos, planos entre otros.
- Testimonial: Consiste en obtener información apropiada de las personas que tienen los conocimientos dentro y fuera del organismo bajo auditoría.

- Analítica: consiste en la ejecución de cálculos, comparaciones, razonamientos, estudio de índices y tendencias, investigación de variaciones y transacciones no habituales.

Al finalizar esta etapa se debe confeccionar una Matriz de Hallazgos (ANEXO IV) que reúne de manera estructurada los principales elementos encontrados en la auditoría.

En esta matriz, además de los hallazgos, son importantes las causas que los originan, y los efectos que pueden producir.

La confección de esta matriz marca la finalización de la etapa de ejecución de la auditoría.

III – B - 3 – Proyecto de Informe

Terminada la etapa de ejecución y a partir de la matriz de hallazgos se redacta el Proyecto de Informe de Auditoría.

De acuerdo a la Resolución N° 26/15 – AGN el informe de auditoría deberá contener las siguientes secciones

1) **Título:** identifica al trabajo realizado.
2) **Receptor:** Autoridad responsable del organismo auditado.
3) **Identificación del objeto de auditoría:** define con precisión el sujeto y la materialidad del trabajo de control.
4) **Descripción de las responsabilidades:** describe la responsabilidad de del controlado y la que le corresponde a la AGN con respecto al objeto.
5) **Alcance:** debe indicar:
    a. Que el trabajo se realizó conforme a las normas propias de la AGN.
    b. Fecha de finalización de tareas de campo.
    c. Los criterios definidos.
    d. Procedimientos aplicados.
    e. Limitaciones al alcance.
6) **Hallazgos:** en la cantidad de apartados necesarios, deberán estar fundamentados en la evidencia recolectada, en la materialidad y en su importancia relativa.
7) **Recomendaciones:** deben servir como base para realizar las tareas correctivas necesarias para superar los hallazgos encontrados.

Cada una de las hojas del proyecto de informe deberá contener la leyenda "Información Estrictamente Confidencial".

III – B – 4 – Comentarios del Auditado

El Proyecto de Informe debe ser enviado al auditado con el fin de que realice los descargos que crea necesario sobre los hallazgos encontrados y las recomendaciones expresadas en el Proyecto de Informe de Auditoría.

Recibida la respuesta del auditado, ésta debe ser analizada cuidadosamente y en los casos que se adjunte información no suministrada anteriormente debe ser sometida a los mismos procedimientos utilizados en la auditoría.

El análisis de la respuesta del auditado debe exponerse mediante una tabla en la cual se muestran el hallazgo, la respuesta del auditado, y los comentarios de la AGN sobre la respuesta, indicando si la respuesta mantiene el hallazgo o se levanta total o parcialmente el mismo.

III – B – 5 – Conclusión

El informe de auditoría se cierra con las conclusiones. En ellas deben resumirse cada uno de los hallazgos encontrados, los procedimientos aplicados, y las cuestiones más relevantes de la tarea realizada. En este punto, la redacción debe ser simple de comprender, completa y autosuficiente.

Debe contener información relevante, mencionando los hallazgos con los fundamentos y evidencias que lo sustentan.

III – B – 6 – Informe de Auditoría

El producto de un trabajo de auditoría es el informe. Por medio de él se comunican los resultados al auditado.

El informe debe ser:

1. Completo: debe incluir toda la información necesaria que dé respuesta a los objetivos de la auditoría.
2. Convincente: debe estar estructurado en forma lógica y ordenada, para vincular fácilmente cada uno de los hallazgos con la evidencia que lo sustenta y la recomendación correspondiente.
3. Oportuno: Debe permitir a los legisladores indicar al organismo auditado lo que debe cumplir para mejorar la situación encontrada. Para esto debe emitirse en una

fecha lo más cercana posible al fin de las tareas de campo, con el fin de que la opinión expresada esté vigente al momento de la publicación.

4. Comprensible: Debe estar escrito siguiendo las Pautas de Estilo y Lenguaje Llano aprobado por el Colegio de Auditores, para que un ocasional lector pueda comprenderlo sin la necesidad de tener que recurrir a expertos que lo interpreten.
5. Objetivo: Debe ser imparcial tanto técnicamente, como políticamente.

La estructura del informe debe incluir:

1. El objeto de la auditoría.
2. Objetivos de la auditoría.
3. Criterios y sus fuentes.
4. Alcance.
5. Período auditado.
6. Limitaciones al alcance.
7. Hallazgos encontrados.
8. Recomendaciones.
9. Comunicaciones al Ente Auditado.
10. Conclusiones.
11. Fecha.
12. Firma.
13. Anexos (si los hubiere).

III – B – 7 – Seguimiento de una Auditoría

Esta etapa del ciclo de vida de la auditoría no es obligatoria en todos los casos. Consiste en un análisis posterior sobre las medidas correctivas adoptadas por el auditado para cumplir con las recomendaciones recibidas oportunamente.

Es importante destacar que solamente serán motivo de análisis los puntos vinculados estrictamente con los hallazgos de la auditoría realizada, no pudiéndose agregar observaciones nuevas.

Procedimientos de Auditoría

Introducción

Los procedimientos enunciados no constituyen un conjunto cerrado de pruebas a realizar; éstos deberán ser complementados con pruebas sustantivas que el equipo decidirá en función del objeto de auditoría.

Análisis de Organización y Políticas del Ente

Estructura Organizacional

Análisis de la Estructura General del Organismo. Misiones y Funciones.

A partir del organigrama del ente a auditar, y de las misiones y funciones definidas para cada una de las áreas, se determinan cuáles son las responsables directas de las principales actividades y las afectadas directamente por la auditoría.

Ubicación del Área de TIC dentro del Organismo. Misiones y Funciones

A fines de verificar el ambiente de control interno se analiza la ubicación de la Unidad de Auditoría Interna dentro del organigrama del ente auditado y su dependencia funcional. Esto permite determinar la independencia del área responsable del control.

Funciones Organizacionales

Administración de RR.HH. de TIC.

Verificar que estén definidos los roles y responsabilidades del personal.

Evaluar los procedimientos de incorporación de personal de TIC, verificando que:

- Estén alineados con los procedimientos generales de la organización.
- Garanticen la igualdad de oportunidades, evitando cualquier tipo de discriminación principalmente política y de género.
- La elección se realice tomando en cuenta sólo las habilidades de los postulantes para el cargo propuesto.

Verificar que el personal haya cumplido con todos los procedimientos administrativos de la organización.

Verificar que existan y se encuentren firmados por todos los empleados del organismo los documentos de "Uso responsable de los recursos informáticos" y "Políticas de confidencialidad de la información".

Verificar la existencia y cumplimiento de un plan de capacitación que permita mantener actualizadas las habilidades y competencias del personal de TIC.

Verificar que estén definidas y se cumplan periódicamente los procedimientos de evaluación de desempeño. Comprobar que el personal cumpla con las metas del organismo y responsabilidades derivadas de su puesto. Verificar que los resultados de las evaluaciones sean tenidos en cuenta para el diseño de los planes de capacitación anual.

Verificar que exista una adecuada segregación de funciones y de responsabilidad, de forma de evitar el riesgo que se apliquen cambios no autorizados, controlando los permisos de acceso de los empleados, especialmente los de las áreas de sistemas.

Administración de Calidad

Verificar que esté formalmente definida y exista un área de aseguramiento de calidad (QA – Quality Assurance).

Verificar que exista y se encuentre aprobada una Política de Calidad para toda la organización.

Verificar que exista y esté formalmente aprobado un Sistema de Gestión de Calidad (QMS – Quality Management System).

Verificar que el Sistema de Gestión de Calidad defina la estructura organizacional incluyendo los roles, las responsabilidades y las tareas a realizar vinculadas con el aseguramiento de la calidad.

Verificar que el Sistema de Gestión de Calidad identifique los requerimientos, los criterios de calidad y los procesos claves de TIC.

Verificar que el sistema de Gestión de Calidad contenga procesos y métodos para definir, detectar, corregir y prever no conformidades.

Verificar que se encuentren definidos indicadores de desempeño relevantes que permitan evaluar la eficacia y la eficiencia de los procesos de la organización.

Verificar que se realicen informes periódicos y sistemáticos que reflejen el grado de desempeño.

Verificar que existen y se realizan acciones correctivas en los casos en que se detecten desviaciones en los indicadores de desempeño.

Verificar que se encuentre definido un marco de trabajo de monitoreo que defina la metodología a aplicar y los procesos a seguir.

Verificar que se encuentren definidos los objetivos de desempeño e identificar los datos que permitan evaluar si estos objetivos se cumplen.

Verificar que se encuentren definidos los procesos de recolección de información de forma tal que la misma sea precisa y oportuna.

Verificar que exista un procedimiento que permita comparar el desempeño con las metas fijadas por la organización.

Administración de Riesgos de TIC.

Verificar que exista y se utilice un marco de administración de riesgos para el organismo.

Verificar que exista un marco de administración de riesgos de TIC alineado con la administración de la organización.

Verificar que se encuentren identificados todos los riesgos, tanto internos como externos, a los que está sometida la organización, y que los mismos fueron evaluados correctamente en cuanto a su impacto y su probabilidad de ocurrencia.

Verificar que se adopten medidas adecuadas para la mitigación de los riesgos identificados.

Verificar la existencia de un Plan de Monitoreo de Riesgos que permita mantener la información de los mismos actualizada de manera que se desarrollen procedimientos proactivos para la mitigación de riesgos.

Administración de Proyectos

Análisis de Ciclo de Vida

Verificar que exista un modelo de arquitectura de información para toda la organización.

Verificar que exista un diccionario de datos, con las correspondientes reglas de sintaxis y esquema de clasificación en función de su criticidad y sus niveles de seguridad.

Verificar que el modelo de arquitectura sea aplicado tanto en el desarrollo de nuevas aplicaciones como en las modificaciones de los sistemas existentes.

Examinar qué aplicaciones no cumplen con el modelo de arquitectura aprobado.

Verificar que el modelo de arquitectura de la información garantice la integridad y consistencia de la misma.

Verificar que fue asignada la propiedad de todos los datos del modelo.

Verificar que exista y se aplique un modelo de ciclo de vida de desarrollo de sistemas que defina cada una de las etapas del mismo, los recursos a utilizar, los entregables y la documentación que debe generar el proyecto.

Metodología de Desarrollo de Sistemas

Diseño y Desarrollo

Verificar que exista un método formal para el desarrollo de sistemas.

Verificar que se complete toda la documentación exigida por la Metodología de Desarrollo de Sistemas.

Verificar que exista un proceso formal de captura de requerimientos, tanto para nuevos desarrollos, como para cambios de los sistemas existentes.

Verificar que cada requerimiento sea aprobado por la instancia que corresponda.

Verificar que los requerimientos de nuevos desarrollos y cambios solicitados sean aprobados formalmente.

Verificar que el diseño sea aprobado por quien lo haya solicitado.

Verificar que exista un entorno de desarrollo totalmente separado de los de testing y producción.

Testing y Aseguramiento de la Calidad (QA – Quality Assurance)

Verificar que exista y se cumpla un plan de pruebas que cubre todo el ciclo de vida de desarrollo de sistemas adecuado a la metodología utilizada.

Verificar que el área de testing cumpla con todas las pruebas descriptas en el plan de pruebas.

Verificar que en el caso que para las pruebas sea necesario utilizar copias de las bases de datos productivas, se enmascaren los datos para asegurar su confidencialidad.

Verificar que exista una aprobación formal del nuevo sistema o modificación del existente por parte de quien lo haya solicitado antes de poner el mismo en producción.

Operaciones

Verificar que exista un documento que describa todos los procedimientos operativos disponibles para aquellos usuarios que los necesiten.

Verificar que los entornos de pruebas y producción estén adecuadamente separados.

Verificar que sólo el personal autorizado accede al entorno de producción.

Mantenimiento y Soporte.

Verificar que exista y se cumpla un procedimiento de gestión de cambios para los sistemas e instalaciones de infraestructura.

Verificar que todos los requerimientos de soporte son identificados en forma univoca.

Verificar que exista una adecuada escalabilidad en la resolución de incidentes.

Verificar que el usuario que inició el requerimiento sea quien apruebe y de conformidad a la resolución del mismo.

Análisis de la Seguridad de la Información

Políticas de Seguridad de la Información

Verificar que exista y se encuentre formalizada la Política de Seguridad de la Información.

Verificar que la Política de Seguridad de la Información haya sido puesta en conocimiento de todos los empleados de la organización y agentes externos que estén vinculados con los sistemas informáticos internos.

Verificar que la política de seguridad sea revisada y actualizada en forma planificada a intervalos regulares, o cuando el avance de la tecnología así lo requiera.

Verificar que se encuentren definidas adecuadamente las responsabilidades de la seguridad de la información

Verificar que el área de seguridad de TIC dentro de la organización reporte directamente a la alta gerencia, sin depender de las áreas de sistemas o de otras a las que deba controlar.

Verificar que todos los empleados del organismo y los terceros que tengan accesos a sus sistemas hayan firmado un acuerdo de confidencialidad o de no divulgación de la información a la cual acceden por razones laborales.

Verificar que existan y se realicen campañas de concientización del personal sobre seguridad de la información.

Los acuerdos con otras organizaciones que involucren el acceso, procesamiento o gestión de la información almacenada en el organismo deben incluir como mínimo todos los requerimientos de seguridad que el organismo tiene para el manejo propio de la información.

Verificar que se haya realizado una adecuada clasificación de los datos que tenga en cuenta la seguridad de los mismos considerando los requerimientos legales, su sensibilidad y criticidad. Dicha clasificación deberá tener como mínimo tres niveles (básico, medio y crítico).

La clasificación de los datos en función de su seguridad debe incluir al responsable de cada uno de ellos. Éste tendrá la potestad de permitir o no el acceso a los datos que sean solicitados desde otras áreas.

Verificar que los usuarios de los sistemas informáticos sólo puedan acceder a los datos que estén autorizados a conocer.

Verificar que exista un marco de análisis para la identificación de los riesgos que puedan afectar a la información del organismo.

Gestión de Usuarios.

Verificar que se encuentren formalmente definidos los roles y responsabilidades en materia de seguridad para todos los empleados del organismo y para terceros que tengan acceso a los sistemas informáticos.

Verificar que existan y se cumplan procedimientos debidamente formalizados para las altas, bajas, modificaciones y cambios de los usuarios de los sistemas de la organización

Realizar un contraste entre listados de personal que dispone el área de recursos humanos y de usuarios de los sistemas con el fin de analizar si presentan inconsistencias.

Verificar que exista y se cumpla un proceso de altas, bajas y modificaciones de permisos de acceso a los sistemas o datos del organismo, que tenga en cuenta la clasificación de los datos en función de la seguridad. En dicho proceso mínimamente debe constar la aprobación del superior inmediato que preste conformidad al mismo.

Verificar que el procedimiento de reautenticación de usuarios tenga los mismos requerimientos en materia de seguridad que para el de alta de usuarios.

Verificar que el sistema imponga el cambio de contraseña en el primer uso o luego de haber reautenticado al usuario.

Verificar que sistema no permita la reutilización de las últimas contraseñas del usuario.

Verificar que el sistema tenga un límite de intentos fallidos.

Verificar que el sistema indique al usuario la cantidad de intentos fallidos.

Verificar que el sistema cierre o suspenda la sesión luego de un tiempo predeterminado, obligando al usuario a autenticarse nuevamente transcurrido ese lapso.

Verificar que las contraseñas caduquen periódicamente de acuerdo a lo establecido en las Políticas de Seguridad de la organización.

Elementos de Seguridad Lógica

Verificar que se encuentren instalados todos los parches de seguridad de los Sistemas Operativos y que exista un procedimiento formalizado que asegure su inmediata instalación cuando los mismos se publican.

Verificar a partir del esquema de la red de datos que exista un efectivo aislamiento del tráfico en la red de acuerdo a lo establecido en la Política de Seguridad.

Verificar que el dimensionamiento de la red de datos es el adecuado y que exista un nivel de redundancia adecuado.

Verificar que los antivirus, antispam y firewalls se encuentren actualizados y se controle su capacidad de detección.

Verificar que los contratos con los proveedores de antivirus, antispam y firewalls se encuentren vigentes y que se dispone de procedimientos formalizados para su actualización.

Verificar que la configuración del firewall o de la DMZ permita solo el tráfico autorizado.

Verificar que se realicen test de penetración (Penetration Test) que verifiquen que solo se encuentren habilitados solamente los puertos y servicios necesarios. Y que en la misma prueba se realice un escaneo y explotación de vulnerabilidades.

Seguridad Física

Verificar que la ubicación del centro de procesamiento sea adecuada y minimice el efecto de posibles desastres naturales que puedan poner en riesgo la continuidad de las operaciones del mismo.

Verificar que desde el exterior no pueda ser identificado el centro de procesamiento, con el fin de dificultar posibles ataques al mismo.

Verificar que se encuentre definido un perímetro de seguridad al cual sólo puede acceder el personal debidamente autorizado, quedando registrada en forma inequívoca el acceso al mismo.

Verificar que, en el caso que sea necesario el ingreso de personal ajeno al área segura, el mismo quede debidamente registrado y esté acompañado en todo momento por personal que tenga los permisos adecuados.

Verificar que los de los racks de comunicaciones distribuidos dentro del organismo (fuera del área segura del centro de procesamiento de datos) se encuentren cerrados con llave y en lo posible fuera del acceso de personal no autorizado.

Verificar que los cableados de energía eléctrica y de comunicaciones se encuentren protegidos de intercepciones o daños.

Verificar que estén definidos y se cumplan todos los procedimientos de mantenimiento preventivo, y que en los casos en que este servicio sea contratado a un proveedor externo el/los contrato/s correspondiente/s se encuentre/n vigente/s.

Verificar que exista un procedimiento formalmente definido y se cumpla para las bajas de equipos que contienen elementos de almacenamiento. El procedimiento debe asegurar que estos elementos fueron retirados o sobrescritos a fin de eliminar cualquier dato sensible.

Verificar que exista, se encuentre aprobado y se mantenga actualizado un Plan de Continuidad de Servicios (DRP – Disaster Recovery Planning). Verificar que se realicen pruebas del mismo con una periodicidad adecuada.

Análisis de Infraestructura

Datacenter

Controles Ambientales.

Verificar que la iluminación centro de procesamiento sea la adecuada para realizar trabajos en el mismo.

Verificar que se controle y registre la temperatura del centro de procesamiento.

Verificar que los Sistemas de Aire Acondicionado posean sus contratos de mantenimiento vigentes, que se cumplan con los trabajos de mantenimiento preventivos previstos, que queden registradas las salidas de servicio no planificadas y que se monitoreen las condiciones establecidas en el acuerdo de nivel de servicios correspondiente.

Verificar que se controle y registre la humedad ambiente dentro del centro de procesamiento y que exista un procedimiento en el caso de que la misma no esté dentro de los rangos aceptados.

Sistemas de Energía

Verificar la instalación del/los o los alimentador/es eléctricos principales. Evaluar que la potencia suministrada por la red eléctrica sea adecuada a la potencia instalada en el centro de procesamiento más una reserva para futuras instalaciones.

Verificar la existencia y el mantenimiento de sistemas de alimentación eléctrica secundaria, sistemas de energía ininterrumpida (UPS), grupos electrógenos que permitan el normal funcionamiento del centro de procesamiento de datos ante la falta de energía eléctrica por parte del/de los proveedor/es.

Verificar que se cumplan las tareas de mantenimiento preventivo de las UPS, principalmente en sus baterías.

Verificar que se cumplan las tareas de mantenimiento preventivo de los grupos electrógenos, principalmente en lo que hace al tiempo mínimo de funcionamiento en un período determinado (de acuerdo a las especificaciones del fabricante), al cambio de los lubricantes y al control del combustible.

Sistemas contra Incendios.

Verificar que el centro de procesamiento de datos cuente con un sistema de detección y extinción de incendios.

Verificar que se cumplan con las tareas de control y mantenimiento periódicas del sistema de extinción de incendios de acuerdo a las especificaciones del fabricante. Se

debe poner especial cuidado en el control de la carga del gas utilizado como elemento extintor, y la verificación de los elementos sensores de humo y temperatura.

Enlaces de Comunicaciones.

Verificar que exista dentro del organigrama un responsable de los enlaces de comunicaciones, tanto internas como externas, y que sus misiones y funciones están correctamente definidas.

Verificar que las responsabilidades de quien está a cargo de las comunicaciones no se superpongan con el responsable de la seguridad. Ambas funciones deben estar correctamente segregadas.

Verificar que exista y se mantenga actualizado un inventario de equipos de comunicaciones.

Verificar que exista un proceso de gestión de equipos de comunicaciones que detalle los procedimientos de alta, modificación y baja.

Verificar, en el caso que la infraestructura sea compartida, que el área de comunicaciones gestione tanto las redes de datos, como las de voz.

Red Interna.

Verificar el esquema de la red interna.

Verificar que dentro de las políticas de seguridad se especifiquen los procedimientos de conexión de equipos a la red.

Verificar que exista un procedimiento que controle que los equipos de terceros que se conectan a la red interna (smartphones, tablets, notebooks) cumplan con los esquemas de seguridad exigidos.

En el caso que no pueda asegurarse que los equipos de terceros cumplan con los requerimientos de seguridad exigidos, verificar que los mismos se conencten a un segmento de red especialmente protegido cuyo tráfico esté limitado a lo estrictamente necesario.

Verificar que la configuración de Switches y Routers sea la adecuada.

Enlaces Externos

Verificar que todos los contratos con las empresas proveedoras de servicios de comunicaciones se encuentren vigentes y estén alineados con la normativa vigente para los mismos.

Verificar que los contratos con las empresas proveedoras establezcan acuerdos de nivel de servicios adecuados a la criticidad de dichas comunicaciones y que en los mismos se establezcan las penalidades.

Verificar que se midan los parámetros de nivel de servicio establecido en los SLA, y que los casos de incumplimiento de servicio sean debidamente penados tal como está establecido en los contratos.

Verificar que las herramientas informáticas utilizadas para el control de los SLA sean independientes de los proveedores de los enlaces de comunicaciones.

Verificar que exista redundancia adecuada en los enlaces de comunicaciones, en lo posible con distintos proveedoResolución N°

Análisis de Bases de Datos

Verificar que la base de datos cumpla con lo establecido por la Ley 25.326 Ley de Protección de Datos Personales.

Verificar que exista un documento que defina la Arquitectura de la Información y que esté alineado con el Plan Estratégico de TIC.

Verificar que exista y se aplique un diccionario de datos corporativo.

Verificar que exista una adecuada segregación de funciones, controlando especialmente que el personal de seguridad de la información no tenga funciones de administrador de base de datos.

Verificar que exista y se aplique una clasificación de datos en función de las políticas de seguridad aplicadas por la organización y que tenga en cuenta lo establecido en la Ley de Protección de Datos Personales.

Verificar que los permisos de acceso a la base de datos estén limitados solamente al/a los Administradores de Bases de Datos (DBA - Data Base Administrator) y a las aplicaciones que utilizan los datos.

Verificar que los usuarios puedan acceder (a través de las aplicaciones correspondientes) solamente a los datos autorizados por su perfil.

Verificar que exista y se cumpla una Política de Copias de Restauración de las bases de datos. En la misma deben especificarse los procedimientos de copias de los datos que contienen las bases y de las estructuras de las mismas.

Verificar que se realicen pruebas de restauración en forma periódica.

Verificar los procedimientos de preparación, autorización, recopilación de los datos de entrada.

Verificar la facilidad de uso de las interfases de entrada.

Verificar los procedimientos de corrección de datos ingresados erróneamente.

Verificar la existencia de datos redundantes y duplicados.

Verificar si existen y se aplican procedimientos para el almacenamiento y protección de los documentos fuentes.

Verificar los procedimientos de carga de datos, si son necesarias y se aplican autorizaciones de niveles superiores para la misma.

Verificar que la interfase de entrada de datos no procese los mismos si todos los campos obligatorios no están completos.

Verificar que la interfase de entrada de datos haga una validación mínima sobre los datos a ingresar (imposibilidad de cargar letras en campos numéricos, validación de formatos de correo electrónico, entre otros).

Verificar la frecuencia de las actividades de revalidación de datos.

Análisis del Control Interno

Verificar que se encuentre definido un marco de trabajo de control interno de TIC.

Verificar la eficiencia y eficacia de los controles internos.

Verificar la existencia de excepciones de controles, en el caso que las hubiere analizar las causas y las medidas correspondientes.

Verificar la existencia de controles propios mediante autoevaluaciones por parte de las gerencias de los procesos, las políticas y los controles de TIC.

Verificar que existen controles externos adicionales que completen los realizados por el control interno.

Verificar que se analizan los controles internos de los proveedores de servicios prestados por terceros.

Verificar que se realicen de controles cruzados con el fin de minimizar erroResolución N°

Verificar que existan instancias de doble autorización en transacciones críticas.

Anexos

ANEXO I – Plantilla de Inventario de Recursos

Las siguientes son las tablas que deben completar los organismos con el fin de suministrar el inventario de activos informáticos.

Equipamiento de red

Router, Switch, Hub, Firewall, etc.

Tipo de Equipo (Switch, Router, Hub, Firewall)	Marca / Tipo / Modelo	Tipo de comunicación (Lan - Wan)	Ubicación física	Antigüedad (años)	Indicar si es propio o rentado (indicar proveedor)	Mantenimiento
Switch Ejemplo	3com vaseline switch2928 sfpplus	Lan	CPD libertad	5	Propio	

Información complementaria:
Acompañar plantilla con mapas (gráficos) de las redes Lan y Wan del organismo

Fuente: Departamento de Auditoría Informática

Servidores

De aplicaciones, comunicaciones, correo, file server, etc. Indicar también los storage de almacenamiento y sistemas de backup utilizados

Equipo (denominación que se le asigna en la organización)	Marca / Tipo / Modelo	CPU (procesador y dispositivos)	Memoria central	Sistema de discos / configuración	Antigüedad (años)	Ubicación física	Número de serie	Situación contractual	Virtualización	Sistema operativo y versión/distrib. (si corresponde, un registro por cada uno)	ID servidor virtual (si corresponde, un registro por cada uno)	Aplicaciones que corren, bases de datos y aplicativos
CONTABLE1	IBM X3250 M5	xeon 4C E3-1241v3 3,5Hz	16 GB	2 Discos IBM 81Y9650 de 900Gb c/u SAS 10k 6Gb SS/Hard Drive	2	CPD libertad	456.663	En garantía	Sí	Linux	BUI2032	Correo electrónico
Ejemplo									Sí	Linux	BUI2031	Web corporativa

Información complementaria:
Acompañar plantilla con mapas (gráficos) de la arquitectura de servidores y storage de almacenamiento.

Fuente: Departamento de Auditoría Informática

Recursos Humanos del Área de TI

Número de Legajo	Apellido y Nombres	Cargo (Nombre del Puesto)	Indicar si es de Planta o Contratado	Resumen de Funciones / Responsabilidades y Tareas	Antigüedad en el cargo
18612 Ejemplo	*José Pérez*	*Gerente de Sistemas*	*Planta*	*Coordinar el área de … Administrar la …*	12

Información complementaria:
Adjuntar organigrama del organismo, de la gerencia de TI, misiones y funciones de la gerencia de TI y de cada área de dicha gerencia.
En caso que el área de Seguridad de la Información no estviera en el ámbito de Sistemas, completar la planilla con los datos de sus integrantes y adjuntar la información complementaria.

Fuente: Departamento de Auditoría Informática

Licencias

Sistemas Operativos de Servidores, S.O. de red, Antivirus, Motores de Bases de Datos, aplicativos de seguridad, aplicaciones corporativas, etc. -no incluir ofimática-.

Nombre del Producto	Versión	Total de Licencias adquiridas	Total de Licencias productivas	Vencimiento de las Licencias	Licencias faltantes	Proveedor de referencia para las adquisiciones	Observaciones / Comentarios
Oracle Ejemplo	*11*	*Enterprise*	*250*	*31/12/2018*	*-*	*Oracle*	

Fuente: Departamento de Auditoría Informática

Sistemas Aplicativos

Sistema de Administración y Finanzas, Sistemas Comerciales, Sistemas Productivos, Sistemas de RRHH y Liquidación de Sueldos, Aplicativos específicos de cada Área.

Nombre del Sistema	Versión	Áreas o Gerencias Usuarias	Módulos que componen el Sistema	Cantidad de Usuarios Nominales	Descripción de la arquitectura del sistema: lenguaje de desarrollo (no aplica a enlatados) y motor de base de datos utilizada	Tiene contrato de Soporte y Mantenimiento? (Para el caso de ser un soft de terceros)	Indicar si es desarrollo Propio o un sistema de terceros (Indicar proveedor)	Antigüedad del Sistema	Observaciones / Comentarios
PeopleSoft Ejemplo	*x*	*Adm y Finanzas, Presidencia, ..*	*Tesorería, Ctas por pagar, Ctas por …*	*250*	*BD Oracle*	*Sí*	*Oracle*	*5*	

Información complementaria:
Se requiere acompañar esta planilla con un mapa de aplicaciones (gráfico de nivel 0) indicando la interrelación entre ellas.

Fuente: Departamento de Auditoría Informática

Provisión de servicios de TI

(*SW-HW-SW de base-comunicaciones-servicios,etc*).

Proveedor del servicio (sea interno o externo)	Alcance del servicio contratado	Situación contractual	Vigencia del Contrato (desde - hasta)	Valores acordados por unidad de tiempo	Referente operativo del servicio (Nombre completo, teléfono, e-mail)	SLA	Observaciones / Comentarios
Telefónica Ejemplo	*Enlace pap*	*Sí*	*01/01/2008 - 31/12/2017*	*$2000 / mes*	*José Pérez. 4777-7777. jperez@*	*99,5%, 100 MB*	

Información complementaria:
Se requiere acompañar esta planilla con copia de cada uno de los contratos especificados.

Fuente: Departamento de Auditoría Informática

Procesos Operacionales de la Organización

Nombre del Proceso	Nombre del Módulo al que pertenece el proceso	Nombre del Sistema al que pertenece el proceso	Áreas Usuarias del Proceso (Indicar todo el arbol jerárquico - Direccion/Gerencia/Departamento/ Área)	Cantidad de Usuarios que Utilizan el proceso	Responsable/s operativo del proceso	Breve descripción de los alcances y objetivos que persigue el proceso	Observaciones / Comentarios
Conciliación de Facturas Ejemplo	*Cuentas por pagar*	*People Soft*	*Dirección de Administración Financiera/Gerencia Contable/Pago a Proveedores/Recepción de Facturas*	*4*	*Jefe de Recepción de Facturas*	*Conciliación de Facturas es un proceso que permite minimizar el riesgo del proceso de pago de facturas a sus proveedores de manera ágil y flexible, mediante un proceso que garantiza la validez fiscal así como de las reglas de negocio requeridas, logrando un canal de comunicación confiable con los proveedores que está al módulo contable.*	

Fuente: Departamento de Auditoría Informática

Relevamiento de computadoras de escritorio, notebooks, netbooks, tablet

Marca / Tipo / Modelo	CPU: Procesador y dispositivos	Memoria central	HD: capacidad y -de corresponder- sistema de discos	Aplicaciones que Corren en el Equipo (SISTEMA OPERATIVO, ANTVIRUS y APLICATIVOS CORPORATIVOS)	Antigüedad del equipo (años)	Usuario que tiene asignado el equipo	Nro de Serie	Monitor asociado: Marca Modelo Pulgadas	Área de asignación del equipo
Clon Ejemplo	*i7, USB, HDMI*	*4GB / 4GB*	*HD Serial SATA 500 bg*	*Windows 10. Office 2007. AVG. SIPCAU, MDE.*	*4*	*gomeza, gimenezb, juarezm.*	*90005645*	*Samsung NH7, 17"*	*RRHH*

Fuente: Departamento de Auditoría Informática

Impresoras

Laser, de escritorio, etc.

Marca / Tipo / Modelo	Cantidad de impresiones por minuto	Impresiones por mes	Comentarios	Costo Alquiler Anual	Costo Mantenimiento Anual	Usuario / Área Usuaria	Nro de Serie	Lugar Fisico
Lexmark MS810 láser BN Ejemplo	*18*	*900*	*promedio base anual*	*$ 0*	*$ 2.000*	*RRHH*	*10012323*	*Pasillo de servicio*

Fuente: Departamento de Auditoría Informática

Telefonía

Centrales telefónicas, teléfonos IP, teléfonos digitales, teléfonos analógico, celulares, Telulares.

Indicar si es Central Telefónica, Teléfono IP, Digital, Analógico, Celular, Telular	Marca-Modelo	Usuario	Antigüedad (años)
Central - IP Office 500 Ejemplo	*AVAYA IP Office*	*Operaciones TI*	*2 años*

Fuente: Departamento de Auditoría Informática

ANEXO II – Plantilla de Plan de Auditoría

Plan de Auditoría

Proyecto

Act. Nº XXX/XX

Supervisor: xxxx
Jefe de Equipo: xxxx

El presente Plan de Auditoría se realiza en un todo de acuerdo con el Manual de Control Externo Gubernamental (MCEG), título III.A.1., "Planificación" y las Normas de Control Externo de la Gestión Gubernamental, apartado III.B.1.i. La estructura del presente Plan comprende los puntos enumerados en dichas normas, presentados con una secuencia acorde a la naturaleza de las tareas del Departamento de Auditoría Informática. Dado que la planificación es un proceso dinámico y continuo, podrá sufrir modificaciones en función de las novedades que surjan durante la fase de ejecución.

Análisis preliminar

A continuación, se presenta el relevamiento global de la información relevante sobre el objeto de control, que permitirá comprender los objetivos, criterios y procedimientos que se presentarán más adelante.

Objeto de auditoría (según POA)

Desarrollo.

Marco conceptual

Desarrollo.

Marco normativo e institucional

Desarrollo.

Procesos destacados

Desarrollo.

Materialidad y significatividad

Desarrollo.

Evaluación del control interno de TIC

Como parte de las tareas de relevamiento preliminar, se ha evaluado de modo general el sistema de control interno de la entidad, concentrando los esfuerzos en los procesos TI intensivos. Al respecto, cabe mencionar que:

- El nivel de madurez del SCI asignado por la SIGEN asciende a …
- En cuanto a los informes de auditoría interna, estos destacan …
- De las entrevistas realizadas surge que …
- Por último, cabe destacar que …

En síntesis, …. El riesgo de control se declara en el punto expuesto a continuación.

Análisis de riesgos

Del análisis preliminar hasta aquí expuesto y de tareas específicas realizadas, se han podido identificar los siguientes riesgos:

- *Riesgo inherente del objeto de auditoría*: …

- *Riesgo de control*: …

- *Riesgo de detección*: el presente Plan de Trabajo comprende un conjunto de procedimientos, tanto de cumplimiento como sustantivos, que procuran reducir a un mínimo el riesgo de detección de errores, a los fines de contar con una base razonable para arribar a conclusiones válidas y suficientes. Un detalle de los procedimientos a aplicar puede consultarse en el Anexo 1.

- *Riesgo de fraudes y lavado de activos*: Un riesgo de detección en particular es el de no detectar un fraude. Este riesgo es mayor que el de no detectar un error, por cuanto puede implicar técnicas de ocultamiento o falsificación (más aún en caso de colusión). No obstante, los riesgos de fraude que preliminarmente podrían considerarse son los de: i) …, ii) …, y iii) …. Al respecto, se hará especial énfasis en los procedimientos sustantivos que en el Anexo 1 se declaran como "sensibles" desde este punto de vista. Los resultados que arrojen serán analizados detenidamente a los efectos de considerar el mérito de oportunamente informar a las autoridades sobre la existencia de operaciones sospechosas.

Procedimientos realizados durante la fase de relevamiento preliminar

La información hasta aquí expuesta se basó en los siguientes procedimientos:

- Entrevistas realizadas a: …
- Inspección ocular de: …
- Análisis de la siguiente información suministrada por el auditado: …
- Análisis de la normativa mencionada en 1.3.
- Análisis de los siguientes informes: …

Definiciones

A partir de la información recolectada durante la fase de relevamiento previo, se presenta a continuación la definición del alcance de la auditoría.

Objeto de auditoría (propuesto)

…

Período auditado

Del xx/xx/xx al xx/xx/xx.

Objetivos de Control

A partir del análisis preliminar arriba expuesto, y teniendo en cuenta que este objeto de control fue propuesto por considerarse preliminarmente que …., se declaran a continuación los objetivos generales del trabajo de control a llevarse a cabo, consistentes en evaluar:

- Objetivo 1
- Objetivo 2
- …

Se aclara que no es un objetivo del presente trabajo …

Cuestiones de auditoría

Para cumplir con los objetivos expuestos, se abordarán las siguientes cuestiones de auditoría, que surgen del análisis de riesgos. La matriz de riesgos elaborada se encuentra en el Anexo 1 adjunto.

- Cuestión de auditoría 1: …

- Cuestión de auditoría 2: …
- Cuestión de auditoría 3: …

Las sub cuestiones o sub preguntas podrán ser consultadas en el Anexo 2 adjunto.

Enfoque de auditoría

La auditoría se desarrollará aplicando un enfoque orientado a …

Criterios de Contrastación

A los efectos de arribar a conclusiones objetivas, se enumeran a continuación los criterios que, en general, se utilizarán como parámetros contra los cuales contrastar la situación encontrada. Estos parámetros cumplen con los atributos deseables de relevancia para el trabajo, aceptación general y consistencia con los utilizados en auditorías similaResolución N° En el Anexo 1 del presente Plan se presenta un detalle de los objetivos específicos y sus respectivos criterios puntuales, que surgen de los aquí expuestos.

- Criterio 1
- Criterio 2
- …
- Criterio n

Procedimientos de auditoría

Los procedimientos de auditoría se detallan en una matriz de planificación que expone de modo desagregado:
- los objetivos específicos,
- información requerida y sus fuentes,
- procedimientos de auditoría específicos para obtención y análisis de datos (punto en cuestión),
- eventuales limitaciones con las cuales se podría encontrar el equipo,
- criterio adoptado como marco de referencia, entre otros.

Al respecto, véase Anexo 1.

Plan de trabajo

Recursos humanos a comprometer

Nombre y apellido	Función	Categoría	Profesión	Situación de Revista

Comisiones de servicio previstas
Para cumplir con los objetivos previstos ….

Cronograma y puntos de control
Porcentaje de avance a la fecha: xx/xx/xx, xx%
Fecha prevista para elevación del borrador interno (85%): xx/xx/xx
Fecha prevista para elevación del borrador sujeto a discusión (89%): xx/xx/xx

Anexo 1. Matriz de riesgos

Insertar matriz de riesgos (Se construye a partir de la expuesta en la Ilustración 17, página 89)

Anexo 2. Matriz de planificación

Insertar matriz de planificación

ANEXO III – Detalle de la Matriz de Planificación

Cuestión de Auditoría: Tema bajo estudio						
Subcuestión de auditoría	**Informaciones requeridas**	**Fuentes de información**	**Procedimientos de recopilación de datos**	**Procedimientos de análisis de datos**	**Limitaciones**	**Qué va a permitir decir el análisis – criterio**
Descomposición del tema bajo estudio en puntos específicos.	Identificar la información necesaria para responder la pregunta de la subcuestión de auditoría.	Identificar el origen de la información necesaria.	Identificar los métodos que se van a usar.	Identificar las técnicas que se van a usar en el análisis de la información y describir los respectivos procedimientos.	Especificar las restricciones en cuanto a problemas en el acceso a las personas y a la información, calidad de la información, condiciones operativas para desempeñar el trabajo.	Precisar que conclusiones o resultados pueden alcanzarse.

ANEXO IV – Detalle de la Matriz de Hallazgo

Hallazgos					Buenas Prácticas	Recomendaciones	Beneficios Esperados
Situación encontrada	Criterio	Evidencias y análisis	Causas	Efectos			
Contrastaciones más relevantes identificadas en la fase de ejecución.	Estándar usado para determinar si el objeto auditado alcanza, excede o está por debajo del desempeño esperado.	Resultado de la aplicación de los métodos de análisis de datos y su empleo en la producción de evidencias. De forma resumida deben ser indicadas las técnicas usadas para tratar de la información recolectada durante a ejecución y los resultados obtenidos.	Pueden estar en e marco de las actividades administrativas y operativas del ente auditado o fuera de su control o influencia. La identificación de causas debe estar sustentada en evidencias. Deberán identificarse las posibles medidas que contribuyan a corregir las causas de las debilidades detectadas.	Consecuencias relacionadas con las causas y con los correspondientes hallazgos. Puede ser una medida de la relevancia de los hallazgos.	Acciones identificadas cuya comprobación lleva a buen desempeño. Estas acciones podrán sustentar la propuesta de recomendaciones.	Deben ser elaboradas para tratar de corregir el origen de los problemas diagnosticados. Se debe dedicar el tiempo suficiente para las deliberaciones y la priorización para la solución de los principales problemas.	Mejoras que se esperan alcanzar con la implementación de las recomendaciones. Los beneficios pueden ser cualitativos y cuantitativos.

ANEXO E – FORMULARIO DESCRIPTIVO DEL TRABAJO FINAL DE GRADUACIÓN

AUTORIZACIÓN PARA PUBLICAR Y DIFUNDIR TESIS DE POSGRADO O GRADO A LA UNIVERIDAD SIGLO 21

Por la presente, autorizo a la Universidad Siglo21 a difundir en su página web o bien a través de su campus virtual mi trabajo de Tesis según los datos que detallo a continuación, a los fines que la misma pueda ser leída por los visitantes de dicha página web y/o el cuerpo docente y/o alumnos de la Institución:

Autor-tesista *(apellido/s y nombre/s completos)*	Gutierrez, Sergio Esteban
DNI *(del autor-tesista)*	16131207
Título y subtítulo *(completos de la Tesis)*	Manual de Normas y Procedimientos de Auditoría de TIC Auditoría General de la Nación
Correo electrónico *(del autor-tesista)*	sergioesteban.gutierrez@gmail.com
Unidad Académica *(donde se presentó la obra)*	Universidad Empresarial Siglo 21

Otorgo expreso consentimiento para que la copia electrónica de mi Tesis sea publicada en la página web y/o el campus virtual de la Universidad Siglo 21 según el siguiente detalle:

Texto completo de la Tesis *(Marcar SI/NO)*[1][1]	SI
Publicación parcial *(Informar que capítulos se publicarán)*	

Otorgo expreso consentimiento para que la versión electrónica de este libro sea publicada en la página web y/o el campus virtual de la Universidad Siglo 21.

Lugar y fecha: Buenos Aires, xx / 12 / 2017

Firma autor-tesista **Aclaración autor-tesista**

Esta Secretaría/Departamento de Grado/Posgrado de la Unidad Académica: _____certifica que la tesis adjunta es la aprobada y registrada en esta dependencia.

Firma Autoridad Aclaración Autoridad

Sello de la Secretaría/Departamento de Posgrado

[1][1] Advertencia: Se informa al autor/tesista que es conveniente publicar en la Biblioteca Digital las obras intelectuales editadas e inscriptas en el INPI para asegurar la plena protección de sus derechos intelectuales (Ley 11.723) y propiedad industrial (Ley 22.362 y Dec. 6673/63. Se recomienda la NO publicación de aquellas tesis que desarrollan un invento patentable, modelo de utilidad y diseño industrial que no ha sido registrado en el INPI, a los fines de preservar la novedad de la creación.