Menghi, Ailen Carolina

Pautas para una auditoría de sistemas de información en un contexto mediado por la tecnología con vistas a la calidad de la información

Tesis para la obtención del título de posgrado de Magister en Auditoría

Directora: Perfumo, María Soledad

PAUTAS PARA UNA AUDITORÍA DE SISTEMAS DE INFORMACIÓN EN UN CONTEXTO MEDIADO POR LA TECONOLOGÍA CON VISTAS A LA CALIDAD DE LA INFORMACIÓN

UNIVERSIDAD CATÓLICA DE CÓRDOBA

Universidad Jesuita

FACULTAD DE CIENCIAS ECONÓMICAS Y DE ADMINISTRACIÓN

MAESTRÍA EN AUDITORÍA

PAUTAS PARA UNA AUDITORÍA DE SISTEMAS DE INFORMACIÓN EN UN CONTEXTO MEDIADO POR LA TECONOLOGÍA CON VISTAS A LA CALIDAD DE LA INFORMACIÓN

Trabajo Final conforme a los requisitos para obtener el título de Magister en Auditoría

Maestrando: **Cra. Menghi Ailen Carolina**

Directora: **Mag. Perfumo María Soledad**

Córdoba, 3 de agosto de 2021

Resumen

La actuación de los profesionales en Ciencias Económicas ha sido objeto de numerosas y detalladas regulaciones encontrándose sujeta a muchos estándares de cumplimiento. Sin embargo, existen áreas donde aún no se poseen definiciones ni regulaciones contundentes y donde la delimitación del alcance de la revisión de auditoría se encuentra difuminada y muchas veces es objeto de confusión y desconocimiento. Al estar la tecnología tan presente en todas y cada una de las áreas de una organización, es un requisito fundamental para quien realizará evaluaciones de un sistema de información, estar actualizado en esta temática y conocer los riesgos que todo desarrollo tecnológico trae al proceso de información.

Aunque la introducción de la tecnología no ha afectado a los objetivos del trabajo del auditor, esta sí ha impactado en los mecanismos de control interno de las organizaciones y en las técnicas y procedimientos a ser aplicados para su comprobación y evaluación. En base a ello es que se propone un conjunto de pautas o lineamientos para la auditoría de sistemas de información mediados por la tecnología donde, además de contemplar los factores que incrementan los riesgos y que poseen impacto sobre los procesos y actividades de generación de información, se consideran los aspectos clave a tener en cuenta para el conocimiento del entorno operativo y ambiente de control, de la estructura y universo tecnológico y para la prueba de controles.

Considerar cómo las nuevas tecnologías han modificado el entorno en el cual se desarrolla la auditoría y la manera en que se valida la información bajo esas nuevas condiciones, representa un aspecto importante donde, además, deben contemplarse las falencias de control que se presentan en la gestión informática respecto a la información, la inexistencia de políticas de seguridad de la información y la carencia de un plan de contingencias que asegure la continuidad en las actividades.

Palabras clave: sistemas de información, tecnologías de información, riesgo, auditoría interna, Informe COSO.

Abstract

The performance of professionals in the field of Economic Sciences has been object of numerous and stringent regulations finding itself subject to countless enforcement standards. However, there are areas that still have not been delimited or tightly regulated, and where the determination of the scope during the revision of an audit is blurred and many times object of confusion and lack of knowledge. Since technology is present in each and every part of an organization, it is an essential requirement that whoever carries out the evaluation of the information system be updated about this topic and be knowledgeable about the risks that every technological development might pose to the information processing.

Even though the introduction of technology has not affected the goals of the auditor's job, it has had an impact on the internal control mechanisms of organizations as well as on the techniques and procedures adopted to verify and evaluate the auditor's performance. This is the point of departure to propose a set of rules or guidelines to audit systems of information through the use of technology that not only contemplates the factors that increase the risks and have an impact on the processes and activities that develop information but it also considers the key aspects taken into account to be aware of what the operative setting and environment control as well as the structure and the technological universe and the test control entail.

Bearing in mind how the new technologies have modified the setting in which auditing takes place and the way in which the information gets validated under those new circumstances represents an important aspect; moreover, the control flaws that come up during the technological management of information, the inexistence of information security policies and the lack of a contingency plan that assures the continuation of activities have to be contemplated as well.

Key words: information system, information technology, risk, internal audit, COSO report.

Índice general

1. Índice de siglas y abreviaturas

BIS: British Standards Institute.
COBIT: Control Objectives for Information Systems and related Technology.
COCO: Comité de Criterios de Control de Canadá.
COSO: Committee of Sponsoring Organizations of the Treadway Commission.
CPCECABA: Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires.
CPCECBA: Consejo Profesional de Ciencias Económicas de Córdoba.
FACPCE: Federación Argentina de Consejos Profesionales de Ciencias Económicas.
IAASB: International Auditing and Assurance Standards Board.
IASB: International Accounting Standards Board.
ISO: International Organization for Standardization.
ITGC: Information technology general controls.
JIS: Japanese Industrial Standards.
NIA: Norma internacional de auditoria.
SAD: Sistemas apoyo para la toma de decisiones.
SIA: Sistemas de información administrativa.
SPT: Sistemas de procesamiento de transacciones.
TGS: Teoría general de sistemas.
TI: Tecnologías de la información.

2. Índice de figuras y tablas

3. Capítulo I: Introducción

El avance tecnológico ha tenido un impacto indiscutido en el mundo de la información. La captación de datos, su procesamiento y su desarrollo han crecido a pasos agigantados contribuyendo a la generación de información en niveles impensados y a costos y tiempos cada vez menores. Con el correr de los años, la globalización de los mercados y el amplio desarrollo en las tecnologías de información y telecomunicaciones, han potenciado de manera directa el valor de la misma, pasando de ser solo un producto desarrollado por las organizaciones a ser un insumo fundamental para el cumplimiento de sus objetivos. Sin embargo, la era tecnológica también ha traído aparejado una gran cantidad de riesgos que requieren ser identificados, evaluados y mitigados.

Al igual que cualquier producto generado por una organización, la información también es el resultado de un proceso, el cual posee claras razones para su existencia y necesita ser diseñado, construido, ejecutado y supervisado identificando los responsables de su realización, definiendo los roles en cuanto a su ejecución y estableciendo los lineamientos para la medición de su rendimiento (IT Governance Institute, 2012). Este concepto se encuentra estrechamente vinculado a lo que conocemos como sistemas de información, el cual constituirá el punto de partida de la presente investigación.

A los fines del desarrollo del presente trabajo se buscará llevar a cabo un estudio teórico abocado a la definición de los sistemas de información a fin de comprender el proceso de generación de la información. Para ello, se tomarán como base algunos postulados básicos que han dado origen a la Teoría general de sistemas (en adelante TGS) y que han servido para ubicar a los sistemas en el ámbito de las empresas y organizaciones. A fin de que los sistemas de información cumplan con la razón de su existencia, estos deben generar información susceptible de ser utilizada por la diversidad de usuarios que encuentran en ella una herramienta útil para la gestión, la toma de decisiones y el adecuado desarrollo de sus actividades. En base a ello y teniendo en cuenta algunas definiciones realizadas por organismos de reconocida trayectoria mundial, se buscará comprender el concepto de calidad de la información, para luego proceder con un desarrollo teórico orientado a describir sus atributos, considerando algunas características definidas en la bibliografía consultada, así como por la normativa contable nacional, internacional y otras de gran utilización.

Dado que el control interno constituye un componente clave de los sistemas de información al encontrarse vinculado al proceso de supervisión y evaluación encargado de mantener el correcto y eficiente funcionamiento de los mismos, se llevará a cabo un breve análisis del rol y responsabilidad del auditor interno respeto a la calidad del producto generado por estos

sistemas. Las tecnologías de información dotan de una característica particular al contexto en el cual se desarrollan los distintos procesos de negocio de una organización por lo que se buscarán identificar aquellos riesgos asociados a dichas tecnologías en el marco de la generación de información. Estos riesgos deben ser tenidos en cuenta por el auditor dado que pueden afectar al elemento mínimo en la generación de información (el dato), a la información propiamente dicha y a todas tareas, procesos decisorios y controles implementados por la organización. Finalmente, tomando como marco al informe COSO, al COBIT 4.1 y al COBIT 5 se buscará desarrollar una propuesta encaminada a la definición de un conjunto de pautas para abordar una auditoría de sistemas de información en el contexto mencionado.

3.1. Antecedentes del tema

Los sistemas han sido objeto de innumerables estudios y desarrollos académicos siendo posible encontrar definiciones orientadas a describir sus componentes, objetivos, funciones, características, comportamientos, entre otros. Dichos estudios y desarrollos se encuentran enmarcados en lo que se conoce como TGS, la cual ha tenido como objetivo impulsar una terminología general relativa a los sistemas, desarrollar un conjunto de leyes aplicables a sus comportamientos y promover una formalización de dichas leyes (Cathalifaud y Osorio, 1998). A partir de esta teoría surgen distinciones conceptuales fundamentales que han servido para gran variedad de estudios incluidos los relacionados a empresas y organizaciones que, enmarcadas dentro de los sistemas sociales, contemplan a los conocidos sistemas de información. El concepto de sistema de información ha sido definido por autores como Volpentesta (2004), quién lo concibe como:

> El sistema formal de personas, equipos y procedimientos que, en forma integrada y coordinada, y operando sobre un conjunto de datos estructurados acorde con las necesidades organizacionales, capturan datos, los transforman en información, los almacenan y los distribuyen, a fin de apoyar las actividades de las organizaciones tales como las operaciones, el control, la administración y la toma de decisiones, necesarios para desarrollar la estrategia y lograr los objetivos planteados (p. 183).

Independientemente del entorno en el que se encuentre cada organización, los sistemas de información deben cumplir siempre con el mismo objetivo, aunque serán sus elementos y sus actividades las que mutarán y se modificarán en relación a cada entorno particular. En este punto, Canetti (2007) sostiene que la tecnología juega un papel relevante otorgando una característica distintiva a dicho sistema dado que, de manera constante, abre paso a nuevas formas de captación de datos, de procesamiento, de almacenamiento y de comunicación siendo la rapidez y la agilidad una de sus ventajas principales.

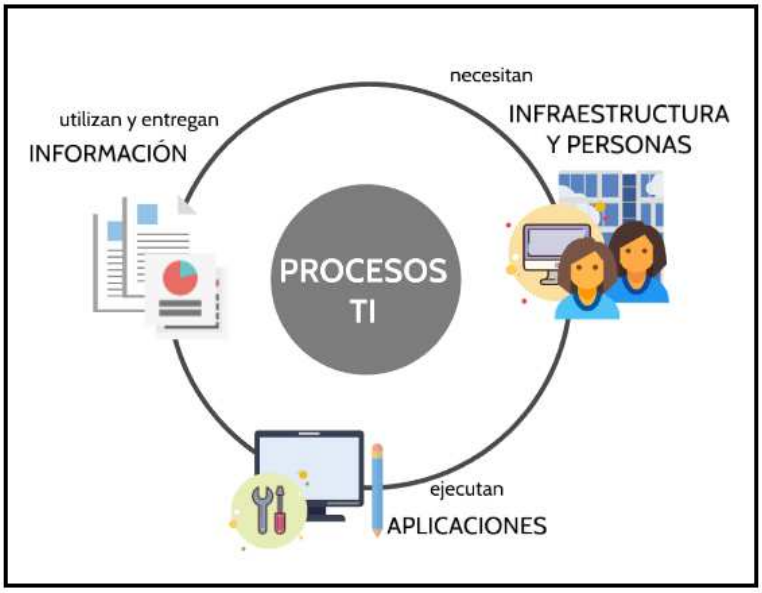
Cuando la tecnología se encuentra orientada a la información y a la comunicación recibe el nombre de tecnologías de la información (TI). Tal como menciona Sal Paz (2010), existe un consenso generalizado en considerarlas como un conjunto de tecnologías que posibilitan la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de la información encontrándose caracterizadas por la automatización, deslocalización, digitalización, diversidad, inmaterialidad, innovación, instantaneidad, interactividad, interconexión y poseyendo mayor influencia sobre los procesos que sobre los productos.

Actualmente es creciente el número de organizaciones que reconocen los beneficios de la tecnología de información y que la utilizan para generar valor para sus partes interesadas. Sin embargo, el éxito en la implementación de estas tecnologías, requiere de una buena administración y de una correcta alineación con los objetivos particulares de cada organización. Para responder a ellos, la organización debe invertir en recursos a fin de crear una capacidad técnica adecuada y que genere los resultados deseados. A tal fin, COBIT 4.1 (IT Governance Institute, 2007) define 4 recursos de tecnología de información que de manera conjunta conforman lo que denomina arquitectura empresarial para TI. Estos recursos son:

1) Aplicaciones: incluyen tanto sistemas de usuario automatizados, como procedimientos manuales que procesan información.
2) Información: son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.
3) Infraestructura: es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
4) Personas: son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a cómo se requieran (p. 12).

De esta forma, y a fin de alcanzar las distintas metas y objetivos establecidos, la organización deberá llevar adelante un conjunto de procesos claramente definidos que utilizarán las habilidades de las personas y la infraestructura tecnológica para ejecutar aplicaciones automatizadas tomando como ventaja la propia información organizativa (IT Governance Institute, 2007).

Figura 3.1.: Arquitectura empresarial TI



Fuente: elaboración propia en base a IT Governance Institute (2007).

De la identificación y definición de estos recursos, podemos observar que la tecnología se halla presente en todas y cada una de las partes de una organización encontrándose los sistemas de información también afectados por dicho fenómeno. Estos sistemas, enmarcados en un contexto mediado por tecnología, son pasibles de amenazas en cada uno de sus elementos y actividades, las cuales pueden afectar a su producto final. La incorporación de datos, la manipulación de los mismos, sus procesamientos, sus salidas, su almacenamiento y su comunicación presentan riesgos que pueden afectar no solo a los activos de información y a sus atributos o características cualitativas básicas, sino que también pueden interferir en una de las metas organizacionales más importantes referidas a la estabilidad o continuidad del negocio o de la actividad.

En la actualidad, cualquier miembro de una organización sabe que la información que es ingresada, generada, almacenada y/o exteriorizada de y por una organización constituye un activo mucho más valioso que todo el equipo que la sustenta. Su valor depende de años de investigación, ideas, cultura, creaciones, pruebas, conceptos y reglamentos (Volpentesta, 2004). Esta información, que ha de ser utilizada no solo para la toma de decisiones sobre una organización, sino que también dentro de ella, debe cumplir con un conjunto de requisitos fundamentales para ser considerada confiable. Sin embargo, lo cierto es que ninguna información puede ser considerada confiable si no se evalúa de manera rigurosa el sistema de información del cual proviene.

Las organizaciones incorporan nuevas tecnologías de la información como componente fundamental de sus sistemas de información con el convencimiento de que la misma puede

mejorar el funcionamiento de la organización, el control de sus procesos y la gestión de sus recursos. Sin embargo, la tecnología considerada de manera aislada y como parte de un sistema de información que no logra alinearse a la cultura y política organizacional, puede llevar al fracaso. La misma, individualmente considerada, es incapaz de generar valor por lo que esta nunca debe constituir un fin en sí misma, sino que debe ser vista como el medio para que el sistema de información del cual forma parte cumpla con el propósito para el cual ha sido creado (Serrano González y Zapata Lluch, 2003).

3.2. Planteamiento del problema

La tecnología en información y las telecomunicaciones han pasado, en muy poco tiempo, de ser un privilegio de unas pocas corporaciones a constituir una necesidad de primer nivel para cualquier organización que se encuentra inmersa en un mundo globalizado. El caudal de actividades que se realizan a diario en instituciones con o sin fines de lucro conjuntamente con los requerimientos externos, lleva a las entidades a *aggiornarse* a los avances tecnológicos, pero como contrapartida siembran un escenario donde el riesgo asociado a la calidad de la información se encuentra latente a lo largo de todo su proceso de generación.

Al estar la tecnología tan presente en todas y cada una de las áreas de una organización, es un requisito fundamental para quien realizará evaluaciones de un sistema de información, estar actualizado en esta temática y conocer los riesgos que todo desarrollo tecnológico trae al proceso de información. Esta, al igual que cualquier otro activo, se encuentra sujeta a una gran variedad de riesgos que no siempre son identificados o percibidos como trascendentales, sino que más bien son considerados menos importantes o marginales. Frente a este nuevo y vertiginoso escenario de riesgo, la auditoría ha sabido encontrar un papel protagónico y de gran responsabilidad donde las políticas de control requieren una adaptación en tiempo real y un necesario enfoque basado en riesgos (CPCECABA, 2013 y Deloitte Touche Tohmatsu Limited, 2018).

Como consecuencia de ello, y dado que la temática tratada es un tema vigente donde día a día se presentan novedosos desafíos como consecuencia de los cambios tecnológicos, el auditor debe identificar y comprender cuáles son aquellos riesgos derivados de la tecnología en el marco de la generación de información, advertir en qué momentos o estadios de este proceso se encuentran y cómo pueden afectar a la información según el momento en el cual se hallan. Adicionalmente, y como consecuencia de que la definición en el alcance de las tareas de revisión frente a estos contextos aún continúa sin tener un desarrollo sólido y contundente, resulta necesario llevar a cabo un proceso crítico de reflexión tendiente a

determinar aquellas pautas que son necesarias considerar en el desarrollo de una auditoría de sistemas de información en un contexto mediado por tecnología.

3.3. Alcances y limitaciones de la propuesta

Por medio del presente trabajo, se buscará brindar herramientas que resulten de utilidad para la auditoría de los sistemas de información abarcando la perspectiva interna y teniendo en cuenta un entorno tecnológico donde el procesamiento electrónico de datos se convierte en el eje fundamental.

Con el propósito de comprender a qué se hace referencia al considerar la perspectiva interna y buscando dotar de un marco conceptual al presente desarrollo, se tomará la definición de control interno establecida por el conocido informe COSO. Al respecto, el Committee of Sponsoring Organizations of the Treadway Commission (2013), define al control interno como:

> Aquel proceso llevado a cabo por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objetivo de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos relacionados con las operaciones, la información y el cumplimiento.
>
> 1) Objetivos operativos: hacen referencia a la eficiencia y eficacia en las operaciones de la entidad, incluidos sus objetivos de rendimiento financiero y operacional, y la protección de sus activos frente a posibles pérdidas.
> 2) Objetivos de información: hacen referencia a la información financiera y no financiera interna y externa y pueden abarcar aspectos de confiabilidad, oportunidad, transparencia, u otros conceptos establecidos por los reguladores, organismos reconocidos o políticas de la propia entidad.
> 3) Objetivos de cumplimiento: hacen referencia al cumplimiento de las leyes y reglamentaciones a las que está sujeta la entidad (p. 3).

Adicionalmente, es importante aclarar que no se pretenderá profundizar en aspectos relacionados con auditoría informática o con auditoría externa de estados financieros. Con el propósito de delimitar el alcance respecto a las auditorías mencionadas, se procede a la definición de cada una de ellas:

- Auditoría externa o de estados financieros:

  Actividad independiente de control retroalimentado y generalmente selectivo de los estados contables de un ente, que compara si las transacciones y el patrimonio incluidos en ellos,

coinciden con la realidad y con las normas contables y comunica los desvíos a la comunidad a través de un informe (FACPCE, 2011, p. 46).

- Auditoría interna:

  Actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización ayudándola a cumplir con sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar los procesos de gestión de riesgo, control y gobierno. La auditoría interna debe evaluar el logro de los objetivos estratégicos de la organización, la confiabilidad e integridad de la información financiera y operativa, el cumplimiento de las leyes, políticas y reglamentos, la eficacia y eficiencia de las operaciones y la salvaguarda de los activos (Pagnone, 2015).

- Auditoría informática:

  Revisión y evaluación de los controles, sistemas y procedimientos de la informática, de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente, confiable y segura de la información que servirá para una adecuada toma de decisiones (Echenique García, 2001, p. 18).

3.4. Objetivos del trabajo y metodología

Objetivo general:

Definir los lineamientos para el desarrollo de una auditoría de sistemas de información en un contexto mediado por la tecnología, a fin de contribuir a la calidad de la información.

Objetivos específicos:

a) Definir qué se entiende por sistemas de información, identificando sus componentes y funciones característicos.
b) Analizar el rol y la responsabilidad del auditor interno respecto a la calidad de la información considerando al control interno como uno de los elementos del sistema de información.
c) Identificar los factores de riesgo que pueden afectar al proceso de generación de la información en el marco del uso de tecnología.
d) Definir las pautas necesarias para el desarrollo de una auditoría de sistemas de información en un contexto mediado por tecnología.

La metodología utilizada para el desarrollo del presente trabajo se basó en una investigación cualitativa por medio de un estudio teórico de tipo clásico (Montero y León, 2007). Se analizaron avances teóricos, estudios de revisión, actualización, comparación y análisis

crítico de diversas teorías o modelos para la definición de lineamientos orientados al desarrollo de una auditoría de sistemas de información en un contexto mediado por tecnología. El trabajo de investigación se abordó como un proceso inductivo, interpretativo, interactivo y recurrente procurando realizar un diagnóstico de la problemática abordada, identificando las categorías sobre las causas y consecuencias de la problemática y la sugerencia de una solución (Hernandez Sampieri y Mendoza Torres, 2018).

La recolección y análisis de datos se apoyó en dos instrumentos y técnicas principales que consistieron en entrevistas y en el análisis documental. A través de ellos se buscó descubrir conceptos y categorías vinculados con la teoría de sistemas, los sistemas de información, los atributos y calidad de la información para la gestión y rendición de cuentas, el rol del auditor en cuanto a dicha calidad y los riesgos derivados de la tecnología en el marco de la generación de información.

Por medio de la investigación documental se identificaron distintos documentos como libros, artículos, glosarios, manuales de buenas prácticas, normas con estándares, guías e informes, que se dispusieron para su lectura e interpretación crítica, sistemática y reflexiva con la finalidad de recolectar, seleccionar, sistematizar, analizar y presentar de modo coherente y comparado las realidades teóricas y empíricas en relación a las categorías de análisis indicadas precedentemente.

Por su parte, las entrevistas fueron estructuradas a partir de los principales problemas identificados como consecuencia de la revisión documental y fueron llevadas a cabo con el objetivo de extraer información relevante a través del análisis de los resultados obtenidos. Si bien se trabajó con una guía temática, las entrevistas se cimentaron sobre preguntas generales, partiendo de un planteamiento global de la temática y dejando que el entrevistado profundice o derive sus apreciaciones más allá de las mismas. Se buscó que los entrevistados puedan manifestar sus experiencias, opiniones, valores, percepciones y creencias sobre los aspectos incluidos en la guía temática. Estos aspectos se resumen en:

1) El conocimiento por parte de las organizaciones sobre los problemas potenciales a ser evidenciados en sus sistemas de información como consecuencia de la mediación tecnológica.
2) Los factores de riesgo que pueden derivar del contexto específico y que requieren ser identificados e incluidos dentro de las actividades tendientes a eliminar o mitigar la probabilidad de ocurrencia de aquellos eventos o acontecimientos que pueden afectar de manera adversa la consecución de los objetivos organizacionales.

3) La percepción que se posee sobre los riesgos derivados de la tecnología en el marco de la generación de información.
4) Los atributos de la información y los efectos que los contextos tecnológicos poseen sobre ellos.
5) Los aspectos críticos a ser considerados al momento de desarrollar una auditoría de sistemas de información teniendo en cuenta el contexto específico.
6) Las evidencias de auditoría y el escepticismo profesional y cómo los mismos se han visto afectadas como consecuencia del contexto específico.

Al seleccionar a los entrevistados se buscó identificar referentes en la temática investigada en el marco de la profesión. Como consecuencia, las entrevistas fueron realizadas a seis profesionales en ciencias económicas especializados en la temática tratada y cuyos ámbitos de actuación se encuentran relacionados con organizaciones de diverso tamaño incluyendo nacionales e internacionales, entidades con y sin fines de lucro y con organizaciones pertenecientes tanto al ámbito público como privado. Por cuestiones de confidencialidad y a pedido de los entrevistados no se mencionan sus nombres ni se hace referencia a sus datos personales y/o laborales.

Finalmente, como consecuencia de los datos y evidencia recolectados por medio de los instrumentos y técnicas mencionados, se procedió con la construcción de lineamientos para una auditoria de sistemas de información mediados por tecnología.

4. Capítulo II: Marco teórico

4.1. Sistemas: de lo general a lo particular

Si escuchamos hablar de sistemas, sus partes, elementos y funciones, probablemente consideremos que sea muy poco lo que podremos sumar a nuestro conocimiento adquirido dado que se trata de un tema muy difundido en la literatura. En el estudio de las ciencias económicas, resulta un concepto bastante desarrollado dado que, a fin de estudiar las organizaciones y su funcionamiento, partimos de la premisa de considerarlas como un sistema que se encuentra inmerso en un sistema de mayor tamaño y del cual se desprenden un conjunto de sistemas más pequeños que son los encargados de llevar a cabo las tareas y actividades que estas necesitan para desarrollarse a lo largo de todo su ciclo de vida.

El concepto de sistemas ha invadido todos los ámbitos de la ciencia llevando a que los mismos conceptos, modelos, leyes y principios surjan una y otra vez en campos diferentes e independientes y teniendo como origen hechos muy diversos. Es a raíz de las grandes similitudes desarrolladas por autores, como Kohler, Lotka, Lewin, Wiener, Shannon y Weaver, Rapoport, Ashby, entre otros, que Bertalanffy se propone aunar los descubrimientos hallados en distintas disciplinas en una gran teoría no desarrollada hasta aquel entonces. Al respecto Von Bertalanffy (1976) afirma:

> Así, existen modelos, principios y leyes aplicables a sistemas generalizados o a sus subclases, sin importar su particular género, la naturaleza de sus elementos componentes y las relaciones o fuerzas que imperen entre ellos. Parece legítimo pedir una teoría no ya de sistemas de clase más o menos especial, sino de principios universales aplicables a los sistemas en general. De aquí que adelantemos una nueva disciplina llamada Teoría general de los sistemas. Su tema es la formulación y derivación de aquellos principios que son válidos para los sistemas en general (p. 32).

El desarrollo de esta teoría, denominada TGS, permitió no solo unir los hallazgos realizados en alejados territorios, sino que abrió paso a un novedoso paradigma. Según su autor (Von Bertalanffy, 1976), el desarrollo de esta teoría tuvo tres pilares primordiales que, sin imaginarlo, sentaron las bases de una nueva era del pensamiento:

1) Ciencia de los sistemas: a partir de esta ciencia surgen principios aplicables a todos los sistemas, la cual surge de la exploración y explicación de este concepto en diversas disciplinas como física, biología, psicología, ciencias sociales, entre otras. Esta nueva esfera del pensamiento toma distancia de la concepción clásica de ciencia

que, a fin de estudiar los distintos elementos de un universo, los aísla, los estudia separadamente y vuelve a unirlos con el objetivo de obtener el sistema o la totalidad. Esta ciencia implanta nuevas bases de análisis donde, a fin de comprender el universo, no solo se requieren los elementos que lo conforman sino también todas las relaciones que existen entre ellos (naturaleza holística).

2) Tecnología de los sistemas: "la tecnología y la sociedad modernas se han vuelto tan complejas que los caminos y medios tradicionales no son ya suficientes, y se imponen actitudes de naturaleza holística, o de sistemas, y generalista, o interdisciplinaria" (p. xiv). Según la concepción de este autor, los problemas que se presentan en algunos sistemas en realidad son problemas de las interrelaciones que se observan entre un gran número de variables. Los requerimientos tecnológicos han conducido a nuevos conceptos y disciplinas que implantan nuevas nociones básicas (como las de las teorías del control y la información, de los juegos y de la decisión, entre otros) pero aunque sus problemas descienden de cuestiones específicas y concretas en tecnología, los modelos, las conceptualizaciones y los principios (retroalimentación, información, control, estabilidad, entre otros) tienen naturaleza interdisciplinaria y resultan independientes de sus campos especiales.

3) Filosofía de los sistemas: representa la reorientación del pensamiento y la visión que resulta de la introducción del sistema como nuevo paradigma científico. Este aspecto se encuentra dividido en tres partes:

- Ontología de sistemas: orientada a definir qué se entiende por sistemas y como se encuentran plasmados en el mundo de las observaciones. La distinción entre sistemas reales y sistemas conceptuales es un ejemplo de los problemas que buscan ser resueltos por este nivel.

- Epistemología de sistemas: referido a los principios, fundamentos y métodos del conocimiento. La TGS se distancia respecto al positivismo o empirismo lógico (neopositivismo) donde el método científico solo es dotado de validez a través de lo empírico o lo verificable prohibiendo la inducción de una regla general a través de observaciones particulares. Para esta corriente, el método científico es la única forma válida de conocimiento (Cathalifaud y Osorio, 1998).

- Filosofía de valores: orientado a las relaciones hombre y mundo. Busca dotar de aspectos humanísticos a una teoría vista como un posible paso final hacia la

mecanización del hombre y hacia una sociedad tecnocrática (Von Bertalanffy, 1976).

El estudio de sistemas tiene una larga trayectoria en el ámbito de la ciencia e incluso, en filosofía y, a pesar de su notada orientación hacia el estudio de la biología y seres vivos, esta teoría ha tenido como objetivo impulsar una terminología general relativa a los sistemas, a desarrollar un conjunto de leyes aplicables a sus comportamientos y a promover la formalización de dichas leyes (isomorfismo de conceptos, modelos y leyes en varios campos). A pesar de sus limitaciones y de su aporte parcial en el mundo moderno, es a partir de ella que surgen distinciones conceptuales fundamentales que han servido para estudios relacionados con ecología, política, psicología, organizaciones y empresas entre otras especialidades antropológicas y sociológicas (Cathalifaud y Osorio, 1998).

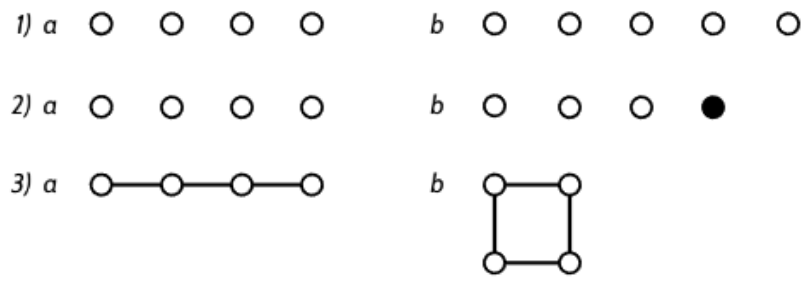
De esta forma, el objetivo de aunar en un bloque contenedor todos los conceptos relativos a los sistemas para ser transformado en un lenguaje universal comienza a encontrar respuesta gracias a disciplinas como la biología donde los esfuerzos de autores como Humberto Maturana y Ludwig von Bertalanffy se encontraron orientados a revestir una teoría universal circunscripta a conceptos y fenómenos de la biología y los seres vivos. Sin embargo, existían otras disciplinas como la sociología, donde se concluía que lo desarrollado en este ámbito no se encontraba lo suficientemente perfeccionado para la explicación de los sistemas sociales. Dado que estos sistemas eran considerados de una complejidad mayor a la que podía absorber el instrumental disponible, autores como Nicklas Luhmann encontraron la necesidad de construir la teoría de sistemas sociales ubicando a la TGS en esta órbita. De esta manera, y con una visión sociológica, este autor despliega énfasis en conceptos referentes a los límites, la función, el medio y las formas, el cierre operativo, la “autopoiesis” (concepto acuñado por Maturana, pero aplicado por Luhmann para los sistemas sociales) y la observación, convirtiendo a su teoría de sistemas en una técnica, instrumento o modo de proceder para el estudio de los sistemas sociales y su perpetuación a través de la comunicación e información (Urteaga, 2010).

Sistemas abiertos, cerrados, datos, entradas (*inputs*), procesos (*throughput*), salida (*outputs*), retroalimentación (*feedback*), entorno, información, entropía, sinergia son algunos de los conceptos que más difusión han tenido en el campo de las organizaciones y empresas, sin embargo, son solo una pequeña parte de la gran teoría que ha ubicado a los sistemas en el ámbito de las ciencias económicas. Es así que, además de la identificación de estos elementos, resulta un punto focal de interés analizar la vinculación existente entre ellos para alcanzar con seguridad el resultado para el cual han sido definidos.

4.1.1. La TGS como punto de partida

"De buenas a primeras, da la impresión de que la definición de sistemas como «conjunto de elementos en interacción» fuera tan general y vaga que no hubiera gran cosa que aprender ella" (Von Bertalanffy, 1976, p. 38). A pesar de que esta breve definición parece no realizar un aporte significativo, a partir de ella se pueden distinguir dos componentes de los cuales es posible desprender un gran abanico de conceptos y explicaciones. El primero de ellos se corresponde con el complejo o conjunto de elementos y el segundo con la interacción o vinculaciones que existen entre dichos elementos. Según Von Bertalanffy (1976), de la conjunción de estos componentes es posible realizar tres distinciones: 1) de acuerdo con su número, 2) de acuerdo con sus especies, 3) de acuerdo con las relaciones entre elementos.

Figura 4.1.: Complejos de elementos



Fuente: Teoría general de sistemas (Ludwing von Bertalanffy, 1976)

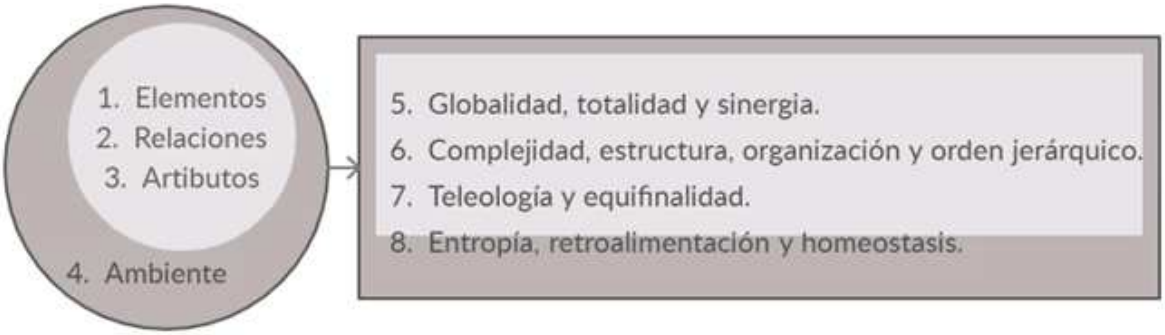
Del análisis de la figura 4.1., donde a y b representan distintos complejos, es posible advertir que existen complejos de elementos con características sumativas y otros complejos con características constitutivas. Las características sumativas se presentan en aquellos casos en donde el conjunto de elementos puede ser entendido como la suma de las partes que lo conforman consideradas de manera aislada. Como consecuencia de ello las características de cada elemento son las mismas tanto dentro como fuera del conjunto. Esto se encuentra plasmado en las situaciones 1 y 2. En cambio las características constitutivas, plasmadas en la situación 3, se presentan en aquellos conjuntos que dependen de los elementos que lo conforman y de las relaciones específicas que tienen lugar dentro del mismo, por lo que no solo es necesario comprender las diversas partes sino también sus relaciones (Von Bertalanffy, 1976). Respecto a ello, el autor concluye:

> El sentido de la expresión algo mística «el todo es más que la suma de sus partes» reside sencillamente en que las características constitutivas no son explicables a partir de las características de sus partes aisladas. Así, las características del complejo, comparadas con las de los elementos, aparecen como «nuevas» o «emergentes». Sin embargo, si conocemos

> el total de las partes contenidas en un sistema y la relación que hay entre ellas, el comportamiento del sistema es derivable a partir del comportamiento de las partes. También puede decirse: si bien es concebible la composición gradual de una suma, un sistema, como total de partes interrelacionadas, tiene que ser concebido como compuesto instantáneamente (p. 55).

Como se indicó con anterioridad, las posibilidades de dominio de los sistemas son numerosas y como consecuencia, también lo son sus propiedades. Las mismas dependen de los sistemas en particular y de las características cualitativas que los identifican y que permiten clasificarlos. Es por ello que a continuación se desarrollan algunos conceptos y principios básicos de esta teoría, que son los que permiten identificar a los sistemas y entender cómo se encuentran conformados. Si bien es posible encontrar una definición unitaria de los mismos, se ha decidido explicar de manera conjunta aquellos conceptos que permiten la compresión de otros o cuando uno de estos lleva a vislumbrar la importancia y la razón de existencia del otro.

Figura 4.2.: Conceptos y características básicas de la TGS



Fuente: elaboración propia.

4.1.1.1. Elementos

Desde un punto de vista estático, los elementos son las partes o componentes que constituyen un sistema. Pueden ser vivientes o no vivientes y es posible encontrarlos en distintas categorías o especies pudiendo ser objetos, conceptos o sujetos. Desde el punto de vista funcional, estos elementos se relacionarán entre sí de manera dinámica y cada uno cumplirá un rol determinado en razón a su funcionalidad. Así es posible distinguir entre elementos de entrada, procesos y elementos de salidas (Schoderbek, Schoderbek y Kefalas, 1984).

La interacción e influencia recíproca entre un sistema y su ambiente se evidencian a través de los elementos de entrada y de salida. Los elementos de entrada constituyen puntos de

partida y son los ingresos que provienen desde el ambiente pudiendo ser personas, energía, datos, materia, entre otros. Estos elementos, a su vez, pueden ser salidas de otros sistemas, pero también es posible encontrar elementos de entradas que formen parte del propio dominio del sistema (Volpentesta, 2004).

Los procesos, por su parte, son aquellas actividades que el sistema aplica sobre los elementos de entrada para introducir cambios en ellos incorporándoles valor y utilidad para transformarlos en elementos de salida. De esta forma, los elementos de salida pueden ser definidos como las consecuencias de los procesos de transformación sobre los elementos de entrada. Consecuencias o resultados que deben estar alineados con los propósitos u objetivos del sistema y que pueden ser servicios, funciones o *retroinputs*. El concepto de *retroinput* no siempre resulta ser un término conocido, sin embargo, es posible asociarlo al de retroalimentación ya que representa a todas aquellas salidas de un sistema que están dirigidas a él mismo en forma de entrada o input (Cathalifaud y Osorio, 1998).

Finalmente, es importante aclarar que un elemento de un sistema puede, a su vez, ser un sistema completo en sí mismo. Este aspecto será tratado mas adelante en el apartado "complejidad, estructura, organización y orden jerárquico" y forma parte de lo que se conoce como orden jerárquico.

4.1.1.2. Relaciones

Las relaciones son los enlaces o las vinculaciones que se verifican entre los distintos componentes del sistema. Estas relaciones representan la interdependencia que existe entre dichos elementos, así como también la vinculación del sistema con su ambiente. Dotan de una característica fundamental a cada sistema ya que gracias a ellas es posible concebirlos como una totalidad superior a la simple suma de sus partes. Las relaciones conectan a los elementos de forma tal que las características del complejo, comparadas con las características de los elementos, aparecen como nuevas o emergentes (Von Bertalanffy, 1976).

Siguiendo a Schoderbek et al. (1984), es posible identificar tres tipos de relaciones dentro de un sistema. Por un lado, existen las relaciones simbióticas que son las que vinculan a aquellos elementos que no podrían funcionar si se encuentran separados o aislados. A pesar de que representan relaciones de vital importancia, son las que poseen menor interés para el investigador dado que su identificación y explicación resultan de gran facilidad. Estas relaciones pueden ser unidireccionales cuando un elemento necesita sí o sí de otro para existir, o bien, bidireccionales cuando ambos se necesitan mutuamente (Volpentesta, 2004).

Por otro lado, encontramos las relaciones sinérgicas que resultan de gran utilidad a fin de mejorar el desempeño de un sistema a pensar de no ser funcionalmente necesarias o vitales. Las relaciones de este tipo son las que permiten tener un resultado superior a la adición de las actuaciones individuales de sus elementos. Finalmente, las relaciones superfluas o de apoyo son aquellas relaciones repetitivas que incrementan la probabilidad de que un sistema opere por mucho más tiempo e incluso en condiciones diferentes a las originalmente planteadas otorgando mayor confiabilidad al mismo (Schoderbek et al., 1984).

4.1.1.3. Atributos

Los distintos elementos que conforman el complejo o sistema y las relaciones que los vinculan poseen determinadas propiedades y características estructurales o funcionales que se denominan atributos. Los mismos pueden referirse a características cuantitativas cuando se centran en cantidades, grados, medidas, etc., o cualitativas cuando están referidas a cualidades, especies, formas, entre otros. Estas últimas suelen estar dotadas de cierto grado de subjetividad razón por la cual resultan más difíciles de medir que las primeras. Adicionalmente es posible clasificar a estos atributos como definitorios cuando permiten designar adecuadamente un elemento o relación o concomitante cuando la presencia o ausencia de este atributo no posee ningún tipo de influencia o carece de importancia (Volpentesta, 2004).

4.1.1.4. Ambiente, límites y frontera

El ambiente es el conjunto de sucesos, condiciones y elementos externos que rodean, contienen e influyen al sistema. Se considera que el ambiente es aquello que impulsa al sistema a adaptarse y reorganizarse configurándose como un proveedor de recursos y convirtiéndose en un medio para su subsistencia, aunque también representando una amenaza (Schoderbek et al., 1984).

A fin de que algo externo pueda ser considerado como ambiente, deben darse dos condiciones: que el sistema no sea susceptible de controlarlo y que este afecte de manera significativa al desempeño y a las propiedades del sistema bajo estudio. Frente a ello es posible encontrar dos clases de elementos del ambiente. Por un lado, los elementos transaccionales, encontrándose representados por todo aquello que el sistema no puede controlar, pero sobre lo que sí puede ejercer influencia (proveedores y consumidores son ejemplos del ambiente de transacciones de una organización) y por otro, encontramos a los elementos contextuales del ambiente que es todo aquello que el sistema no puede controlar

ni modificar (la competencia y los cambios climáticos son ejemplos de este tipo) (Volpentesta, 2004).

Los sistemas consisten en totalidades y por lo tanto son indivisibles. Poseen partes y componentes que son, a su vez, otras totalidades (subsistemas) de forma que entre totalidad y totalidad existen fronteras que demarcan las discontinuidades estrucutrales entre una totalidad y su ambiente. Es posible considearar que un sistema existe dentro de sus límites o fronteras de forma que estos encierran a sus elementos y a las relaciones que existen entre ellos. Todo aquello que se encuentre por fuera de estos límites constituye su ambiente (Cathalifaud y Osorio, 1998).

A pesar de lo expuesto, en la realidad no todas las delimitaciones resultan claras o sencillas. En aquellos sistemas ideales, modelos o no concretos, que se corresponden con construcciones simbólicas donde no existe una percepción u observación directa o que constituyen abstracciones de la realidad, la demarcación de los límites queda en manos del observador de forma que nunca dejan de ser subjetivas o arbitrarias (Volpentesta, 2004). Es importante entender que en aquellos sistemas donde no es posible realizar una delimitación concreta por las propias características del mismo, es la perspectiva intelectual del observador quien fijará esa frontera. Por otra parte, cada problema particular que se presenta en un sistema podría obligar a correr sus límites dando lugar a distintas y nuevas demarcaciones. En estos casos, la fijación de los límites puede presentar una disyuntiva dado que si se fijan de manera muy amplia serán demasiados los elementos y relaciones a considerar dificultando su estudio pero, al restringirse dicho límite, podrán dejarse afuera elementos y relaciones de gran interacción. En ambos casos, las consecuencias podrían conllevar conclusiones o decisiones erradas (Volpentesta, 2004).

4.1.1.5. Globalidad, totalidad, concepto holístico y sinergia

El principio de totalidad parte de las características constitutivas que fueron explicadas anteriormente. El hecho de que un sistema no pueda ser explicado solo por la suma de sus partes, inserta el concepto holístico como referencia para el estudio de sistemas. Un sistema representa una unidad global e indivisible y no simplemente elemental dado que se encuentra constituido por partes vinculadas e interrelacionadas (Cathalifaud y Osorio, 1998).

Una de las principales particularidades de los sistemas, al considerarlos como una globalidad, es la existencia de cualidades que resultan de la integración de sus elementos y que es posible reconocerlas solo en la totalidad constituida superando las características individuales de estos elementos, pero sin que estas últimas sean negadas o minimizadas.

De esta forma, el holismo consiste en que para poder comprender y explicar un sistema es necesario tomarlo como un todo y no reducirlo a sus partes. Al aislar sus partes, solo se logra una visión también aislada que tendrá como consecuncia la pérdida de la verdadera esencia del sistema (Flórez y Thomas, 1993). Reforzando esta afirmación, Volpentesta (2004) añade que, cuando surge un problema relacionado con los sistemas y se trabaja localmente desconociendo o ignorando la globalidad, buscarán aplicarse soluciones inmediatas y concretas que, dado el nivel de complejidad, no llevarán a un adecuado resultado como consecuencia de simples lecturas lineales.

El concepto de totalidad fue tratado y resaltado por Von Bertalanffy (1976) como la característica distintiva y fundamental para el estudio de sistemas y constituye la diferencia principal entre el estudio científico clásico y moderno. Al respecto, sus palabras señalan:

> Es necesario estudiar no solo partes y procesos aislados, sino también resolver los problemas decisivos hallados en la organización y el orden que los unifican, resultantes de la interacción dinámica de partes y que hacen el diferente comportamiento de estas cuando se estudian aisladas o dentro del todo (p. 31).

A partir del concepto de totalidad, es posible entender el concepto de sinergia. “El todo no es igual a la suma de sus partes” es la icónica frase utilizada para describirla. La sinergia es entendida como aquella propiedad común que poseen todos los sistemas y que manifiesta una acción combinada, un esfuerzo cooperativo que permite mejorar sustancialmente el desempeño de un sistema originando un total superior a la simple suma de sus partes consideradas de manera independiente. Todo sistema es sinérgico en tanto el examen de sus partes de manera aislada no puede explicar o predecir su comportamiento (Schoderbek et al., 1984).

4.1.1.6. Complejidad, estructura, organización y orden jerárquico

La complejidad es aquella condición que se encuentra determinada por la cantidad de elementos que componen un sistema (complejidad cuantitativa), por los atributos de dichos elementos (complejidad cualitativa), por sus potenciales interacciones (conectividad), por el nivel de organización implícito y por el número de estados posibles que se producen a través de estos (variedad, variabilidad) (Cathalifaud y Osorio, 1998 y Volpentesta, 2004).

Tomando como referencia a Herrscher, Volpentesta (2004) expresa que la complejidad es la condición que presenta un sistema cuando se dan al menos una de las siguientes situaciones:

> a) que esté conformado por muchos elementos que interactúan de modo no simple; b) que sus causas, efectos o estructura no sean conocidos; c) que necesite mucha energía, tiempo o información para ser manejado; d) que produce efectos que son al mismo tiempo deseados o indeseados, o muy difíciles de controlar (pp. 105-106).

La complejidad de los sistemas sería una de las propiedades analizadas por el economista Kenneth Boulding que, al igual que Von Bertalanffy y de manera independiente, llegaría al desarrollo de su propia teoría de sistemas. Este economista fue el autor de la denominada jerarquía de complejidad estableciendo un orden jerárquico de sistemas partiendo de estructuras simples hasta llegar a las de mayor complejidad. El aporte importante realizado por este autor, consiste en comprender que dentro del mundo de los sistemas existe una jerarquía de forma que un sistema se encuentra conformado por un conjunto de sistemas de menor orden (subsistemas), así como este forma parte de un sistema de orden y complejidad superior conjuntamente con otros subsistemas de igual rango (Navarro, 2001).

La organización, por su parte, se refiere al arreglo de las relaciones, reales o potenciales, entre los distintos elementos del sistema y que conllevan a la conformación de un todo. De esta manera, estos componentes son ensamblados y puestos en acción bajo una forma establecida (Cathalifaud y Osorio, 1998). Por otro lado, el concepto de estructura hace referencia a la organización interna de los elementos. En función de las características cuantitativas y cualitativas de las relaciones entre los componentes, la estructura de un sistema puede alcanzar distintos grados de complejidad por lo que debe ser entendida como una red compleja de interrelaciones y vinculaciones entre las partes y no como una simple serie de relaciones fijas y permanentes (Volpentesta, 2004).

Finalmente, y a modo de comprender claramente las definiciones de dos conceptos afines, citamos a Flórez y Thomas (1993):

> La organización es la que determina que el sistema trabaje de una manera determinada y se dirija hacia cierto punto puesto que su estructura depende no solo de los elementos sino también de las interrelaciones que ocurren al interior inducidas por la organización. La función y la organización aportan las directrices de sostén, de mecánica, de dinámica y de productividad del sistema (p. 24).

4.1.1.7. Teleología y equifinalidad

La conceptualización de un sistema debe comenzar siempre con un objetivo, un propósito o una causa final que puede consistir en una meta, un estado final o una posición de

equilibrio. La búsqueda permanente de dichos objetivos es lo que se denomina teleología (Volpentesta, 2004). Siguiendo este concepto teleológico, Von Bertalanffy (1976), enuncia dos tipos de finalidades y las engloba de la siguiente manera:

1) Teleología estática o adecuación: consiste en una disposición útil para un determinado propósito.
2) Teleología dinámica: consiste en procesos dirigidos u orientados y es posible distinguir cuatro fenómenos: (i) Dirección de acontecimientos hacia un estado final del cual dependen ciertos comportamientos. Todo sistema que alcanza una condición independiente del tiempo se conduce de esta manera. (ii) Dirección basada en una disposición estructural que conduce un proceso o conjunto de ellos de tal forma que permite el logro de determinado resultado. Este tipo de dirección se encuentra regulada por un mecanismo denominado retroalimentación. (iii) Estado final partiendo de diferentes condiciones iniciales y por diferentes caminos (equifinalidad). (iv) Finalidad o intencionalidad, significando que la meta se encuentra inicialmente inserta en el pensamiento y que dirige la acción presente.

La equifinalidad se encuentra ligada al concepto teleológico ya que presupone el deseo o necesidad de llegar a una meta o estado final. Von Bertalanffy (1976) define este concepto de la siguiente manera:

> En cualquier sistema cerrado, el estado final está inequívocamente determinado por las condiciones iniciales. (…) Si se alteran las condiciones iniciales o el proceso, el estado final cambiará también. No ocurre lo mismo en los sistemas abiertos. En ellos puede alcanzarse el mismo estado final partiendo de diferentes condiciones iniciales y por diferentes caminos. Es lo que se llama equifinalidad (p. 40).

La búsqueda permanente del logro de los objetivos, metas o estados finales puede verse como un deseo de continuidad y subsistencia. Todo sistema que posee un comportamiento finalista, es un sistema que busca de manera constante un equilibrio o un estado uniforme. Ahora bien, si en los sistemas abiertos, las distintas condiciones iniciales y los diferentes caminos pueden llevar igualmente al estado final deseado, serán los procesos regulatorios los que ayudarán a alcanzarlo (Flórez y Thomas, 1993 y Castro y Filippi, 2010).

4.1.1.8. Entropía, retroalimentación y homeostasis

El concepto de retroalimentación es, tal vez, uno de los conceptos más controversiales que ha invadido el campo de la teoría de sistemas y encuentra su máximo desarrollo en el ámbito conocido como cibernética, término utilizado para concebir al estudio de los procesos

de comunicación y de control sobre la cual se basa la llamada sociedad de la información (González, 2007).

Desde esta visión, todo ser biológico, artificial o mecánico es un ente informacional y por ende está en su naturaleza el intercambio de información con su ambiente. Así, Wiener (1969) entiende y denomina información:

> Al contenido de lo que es objeto de intercambio con el mundo externo, mientras nos ajustamos a él y hacemos que se acomode a nosotros. El proceso de recibir y utilizar informaciones consiste en ajustarnos a las contingencias de nuestro medio y de vivir de manera efectiva dentro de él. (…) Vivir de manera efectiva significa poseer la información adecuada (p. 17).

Dentro del pensamiento cibernético, al considerar al universo como una totalidad, es posible encontrar una tendencia hacia la desorganización y al caos, tendencia que tiene a incrementarse a medida que crece la edad del universo y haciendo que su condición tienda a empeorar al ir perdiendo sus características distintivas. Esto es lo que se conoce como entropía y se define como una medida de probabilidad de desorden cuya característica fundamental es ser siempre creciente. Esta entropía, al incrementarse, provoca que todo el universo y el conjunto de sistemas que forman parte de él tiendan a empeorar pasando de un estado de organización y diferenciación a uno caracterizado por el caos, la desorganización y el desorden (Castro y Filippi, 2010). De esta forma Wiener (1969) concibe al orden como un estado menos probable y al caos como a un estado naturalmente más probable y ubica a la información como aquello que enfrenta a este estado de desorden buscando reducirlo y tratando de alcanzar aquel que es menos probable:

> Así como la entropía es una medida de desorganización, la información, que suministra un conjunto de mensajes, es una medida de organización. De hecho, puede estimarse la información que aporta uno de ellos como el negativo de su entropía y como el logaritmo negativo de su probabilidad. Es decir, cuando más probable es el mensaje, menos información contiene (p. 21).

Dicho en otras palabras, los mensajes se encuentran constituidos por información y esta por datos, de forma que la información es la organización de un contenido que es objeto de intercambio y que encuentra en la construcción de un mensaje un mecanismo contrario a la entropía (Castro y Filippi, 2010).

Partiendo entonces de un estado no deseado, la información forma parte de un proceso de ajuste y regulación que busca modificar el estado de desorganización más probable para convertirlo en un estado deseado o de mayor organización. Este proceso de ajuste es lo que

Wiener (1969) define como retroalimentación y consiste en el aprovechamiento y uso de la información para controlar o regular una acción y aprender de ella. Al respecto, define al *feedback* o retroalimentación como:

> Un método para regular sistemas introduciendo en ellos los resultados de su actividad anterior. Si se utilizan estos resultados como simples datos numéricos para corregir el sistema y regularlo, tenemos la sencilla retroalimentación de la ingeniería que se ha dado en llamar de control. Sin embargo, si la información que procede de los mismos actos de la máquina puede cambiar los métodos generales y la forma de actividad, tenemos un fenómeno que puede llamarse de aprendizaje (p. 57).

De esta forma, y tal como define su autor, la cibernética representa el estudio de las estructuras de los sistemas reguladores, es decir se propone descubrir los mecanismos presentes en los sistemas que sirven para regular los actos del otro o de sí mismo. Este mecanismo regulador se conoce como retroalimentación negativa o simplemente retroalimentación. Sin embargo, es importante realizar una distinción. El proceso descripto se corresponde con mecanismos que buscan estabilizar o mantener a un sistema dentro de los parámetros deseados. Estos mecanismos se consideran compensadores ya que buscan contener o amortiguar las desviaciones que se presentan. Por otro lado, existe lo que se conoce como retroalimentación positiva que, en contraposición con la negativa, actúa de manera amplificadora de forma que una determinada situación inicial es propagada a lo largo de todo el proceso y se ve reforzada. Este tipo de retroalimentación tiende a no mantener un equilibrio, sino que busca trasladar al sistema a un nuevo estado reforzando la dirección que este ha tomado (Navarro, 2001).

Definidas y explicadas la entropía y el proceso de retroalimentación, nos adentramos en el concepto de homeostasis o equilibrio dinámico para definirlo como aquella propiedad que se expresa a través de la respuesta que un sistema realiza frente a su entorno a fin de lograr su adaptabilidad y en busca de un funcionamiento eficaz (Volpentesta, 2004). La capacidad continua de trabajar no es posible en un sistema cerrado ya que este tiende a alcanzar rápidamente un equilibrio. En los sistemas abiertos se llega a un equilibrio en un tiempo indefinidamente corto pero que no es constante por lo que la búsqueda de dicho equilibrio es permanente. El equilibrio es aquello que busca alcanzarse y no necesariamente se corresponde con un estado (Von Bertalanffy, 1976).

Como expresamos con anterioridad, el sistema se relaciona con su entorno a través de los elementos de entrada y salida. Frente a las variaciones de las condiciones del ambiente, los elementos de entrada pueden desestabilizar el funcionamiento interno del sistema y acentuar su proceso entrópico. Frente a ello, y a fin de asegurar su supervivencia dinámica,

los sistemas requieren de procesos de compensación interna que sustituyan, bloqueen o complementen dichos cambios. Se trata de dispositivos de autocontrol o autorregulación que permiten una adaptación permanente de sus componentes y estructuras (Cathalifaud y Osorio, 1998).

4.1.2. Concepto y definición de sistema

Iniciado el capítulo se tomó una breve definición de sistemas según las palabras del autor de la TGS, de la cual se analizaron sus componentes y algunas características. Definidos los conceptos relacionados a esta teoría, es posible realizar una definición más detallada que permita captar la esencia del concepto de sistemas. Partiendo de Von Bertalanffy con su breve definición y pasando por autores como Laudon y Laudon, Schoderbek, Schoderbek y Kefalas, Cathalifaud y Osorio entre otros, se ha decidido tomar, a los fines de este trabajo, la definición realizada por Volpentesta (2004) quién, a través de la incorporación de algunas de las propiedades comúnmente observables, logra obtener una definición más abarcativa y precisa. Al respecto enuncia:

> Un sistema es un conjunto organizado de elementos interrelacionados que interactúan entre sí, entre sus atributos y con su ambiente conformando una totalidad, persiguiendo un fin determinado, y teniendo una actuación conjunta superior a la suma de las actuaciones individuales de sus elementos (p. 86).

Profundizando en las características que ubican a los sistemas como una globalidad y siguiendo las afirmaciones efectuadas por otros autores, Volpentesta (2004) reconoce cinco condiciones que necesariamente debe satisfacer todo conjunto de elementos que se encuentre encuadrado dentro de la definición de sistemas:

1) Existencia de uno o más atributos o funciones que definan al conjunto.
2) Existencia de un subconjunto de partes esenciales sin las cuales es imposible que se lleven a cabo las funciones básicas. Estas partes se presentan como indispensables pero consideradas por sí solas son insuficientes. Este subconjunto convive, a su vez, con otro subconjunto de elementos no esenciales que, si bien no se consideran indispensables, sí afectan el funcionamiento del sistema como totalidad.
3) Existencia de una conducta individual de cada una de las partes que posee efectos sobre la conducta del todo.
4) La forma en que cada parte esencial impacta sobre el comportamiento de un sistema y sus propiedades, depende del comportamiento o propiedades de la o las otras partes

esenciales de forma que ninguna parte esencial posee un efecto independiente sobre el sistema. Todas se encuentran conectadas de manera directa o indirecta.

5) El efecto de un subconjunto de partes esenciales depende del comportamiento o de las propiedades de otro subconjunto de la misma forma que sucede con las partes individuales. No hay independencia entre ellos.

Finalmente, y a modo de conclusión se considera importante resaltar el papel fundamental que las relaciones juegan dentro de un conjunto. Sin ellas es imposible concebir una totalidad y hacer valer las propiedades que cada una de las partes aportan a un sistema. Cada parte posee una propiedad que se pierden o que resulta inexistente cuando se separa del sistema, así como cada sistema posee propiedades esenciales que no es posible encontrar en alguna de sus partes individuales. La globalidad hace posible la funcionalidad del sistema ya que ninguna parte esencial, por más importante que sea, podrá cumplir por sí misma con la función que define al sistema (Volpentesta, 2004).

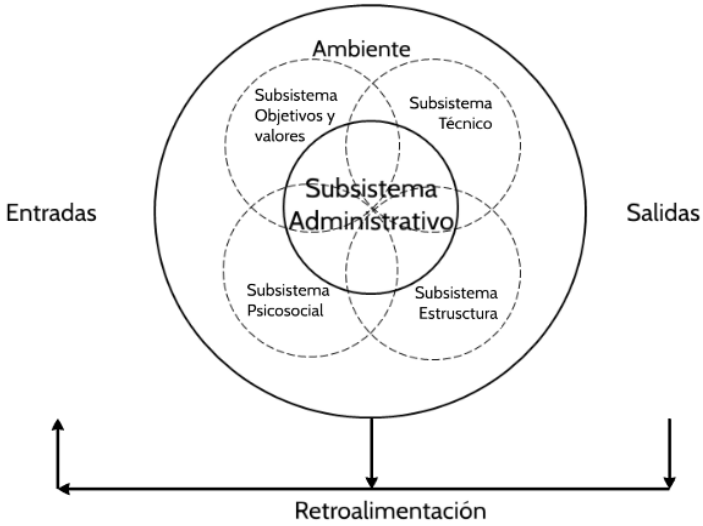
4.2. Las organizaciones y los sistemas

La concepción de las organizaciones como sistemas fue el resultado de años de análisis y analogías. Hasta inicios del siglo XX, las organizaciones (específicamente las empresas) estuvieron encuadradas dentro de modelos deterministas que las denotaban como simples máquinas carentes de objetivos y propósitos propios. Solo existían para cumplir con los objetivos particulares de sus propietarios que estuvieron marcadamente orientados hacia el lucro y las utilidades. Posteriormente, dicha concepción mutó hacia modelos animados donde la analogía con los animales permitió entenderlas y estudiarlas como organismos que poseían vida y propósitos propios orientados a la supervivencia y al crecimiento. En la actualidad, dichas concepciones han evolucionado para ubicarse en los modelos sociales que dejan de lado los comportamientos causa-efecto y los mandatos biológicos que tanto caracterizaron a los modelos anteriores. Las organizaciones pasan a formar parte de los sistemas sociales y a poseer responsabilidades propias con sus integrantes y con el medio que las sustenta quedando inmersas en una familia de sistemas de similares características, pero con diferentes funciones (Volpentesta, 2004).

La jerarquía de sistemas permite entender a las organizaciones como sistemas conformados por componentes que a su vez constituyen sistemas en sí mismos. Siguiendo la estructura social, encontramos un subsistema característico de este tipo de sistemas que es el referido a los objetivos y valores. Este subsistema está relacionado con la cultura, los valores, las creencias y con los objetivos organizacionales, individuales y sociales. Encontramos, como otros componentes, un subsistema psicosocial compuesto por personas, grupos y las

interacciones entre ellos, un subsistema técnico referido a los conocimientos requeridos para las tareas, las técnicas, los equipos y las instalaciones y finalmente un subsistema estructura referido a la división y coordinación de dichas tareas. De la interacción de estos se da origen al subsistema de gestión o administrativo (Volpentesta, 2004). De esta forma es posible esquematizar los subsistemas mencionados de la siguiente manera a fin de conformar una organización definida como sistema sociotécnico abierto.

Figura 4.3.: La organización como sistema socio-técnico abierto



Fuente: Sistemas administrativos y sistemas de información (Volpentesta, 2004).

Las organizaciones como sistemas sociales encuentran su característica distintiva en la conjunción de diversos objetivos que guiarán su accionar. Así buscará no solo la satisfacción de los objetivos organizacionales, sino que también deberá velar por los objetivos individuales de quienes formen parte de la misma y por los objetivos sociales de su contexto. Esta distinta combinación de responsabilidades requiere de una función que dirija todos los procesos que se encuentren orientados a cumplirlos. Esta función se denomina administración y se corresponde con el destino del subsistema administrativo (Volpentesta, 2004).

Los sistemas administrativos han pasado de organizar cosas, a organizar personas para posteriormente orientarse a la organización de la información, convirtiéndose en sistemas responsables de trasformar esa información en un activo valioso que hace posible que las organizaciones aprendan y se adaptan. Un buen sistema administrativo permite procesar gran cantidad de operaciones logrando que se ejecuten en el momento preciso, al menor costo posible, brindando seguridad y generando toda la información que es requerida por los distintos niveles organizativos para la toma de decisiones. La información es generada y se mueve a lo largo de toda la organización por lo que el sistema administrativo dependerá de

ese flujo de información que se organiza bajo un esquema formal dando existencia a una entidad denominada sistema de información. Consecuentemente, y retomando la jerarquía sistémica, ubicamos al sistema de información como un subsistema del administrativo (Volpentesta, 2004).

4.2.1. Sistemas de información

Sabemos que la información es un recurso esencial en toda organización, pero cuando pensamos en ella la imaginamos como algo que simplemente existe por sí misma. Sin embargo, es el resultado de un continuo e ininterrumpido proceso encargado de generarla, comunicarla, exponerla y resguardarla. Ligados al concepto de información encontramos a los datos y al conocimiento que, a pesar de ser conceptos no siempre diferenciables, no resultan ser términos equiparables.

Los datos son un conjunto de símbolos que representan transacciones, acontecimientos y atributos o características de estos. Dentro de una organización los datos representan una gran cuantía y, aunque por sí solos no poseen ningún significado, constituyen la materia prima para la creación de información. De esta manera, la información es el resultado de un proceso que busca dar sentido, forma, significado y valor a un conjunto de datos o a parte de ellos. Además del proceso que separa y diferencia los datos de la información, existe otro componente que los distingue: el receptor. Este debe encontrar en la información algo que no le era conocido con anterioridad, que ayude a reducir su incertidumbre en un momento determinado y que no le sea posible obtener de la simple observación del conjunto de datos existentes. Así como la información deriva de datos, el conocimiento deriva de información. El proceso que permite la transformación de información en conocimiento se denomina aprendizaje y es donde esta se conjuga con la experiencia, los valores y la comunicación organizacional (Volpentesta, 2004).

La información puede obtenerse a través de procesos formales o informales. En los procesos informales no existe un consenso definitorio de información ni se observan comportamientos establecidos para procesarla o almacenarla. Aunque existe una marcada tendencia a no valorizar este tipo de fuente o recurso, en especial las redes de personas sobre la cuales no se producen registros, no implica que los mismos no sean útiles o que resulten menos importantes, el desafío consiste en incorporarlos dentro de los procesos formales para potenciarlos. Por otro lado, los procesos formales son estructurados, poseen definiciones y acuerdos concretos respecto a las actividades a realizar, son explícitos, comunicados, enseñados y adaptados por lo que toda la organización los conoce y sabe

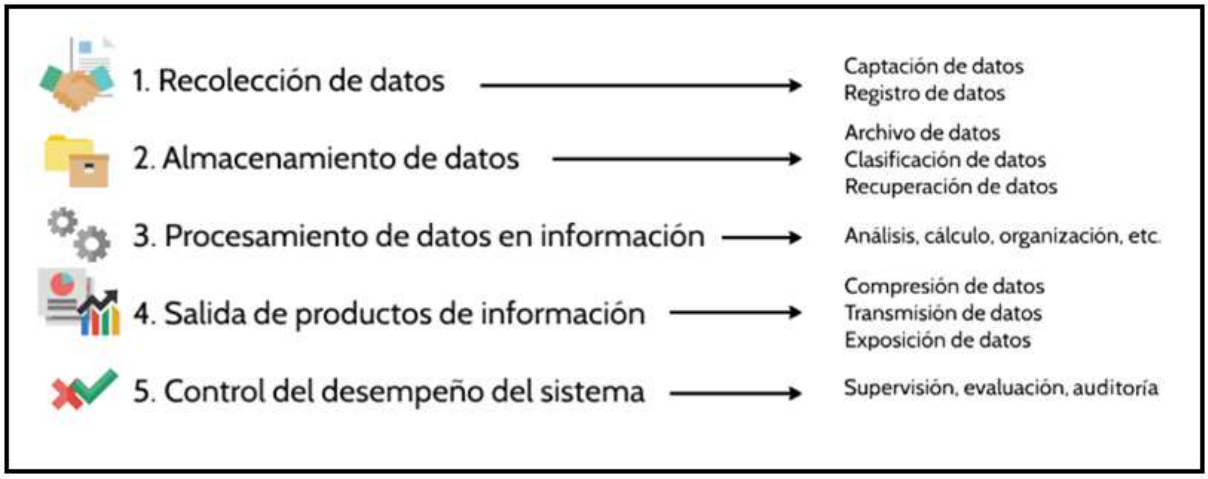
cómo utilizar. Dentro de estos procesos formales encontramos al sistema de información, el cual es definido por Volpentesta (2004) como:

> Sistema formal de personas, equipos y procedimientos que, en forma integrada y coordinada, y operando sobre un conjunto de datos estructurados acorde con las necesidades organizacionales, capturan datos, los transforman en información, los almacenan y los distribuyen, a fin de apoyar las necesidades de las organizaciones tales como las operaciones, el control, la administración y la toma de decisiones, necesarias para desarrollar la estrategia y lograr los objetivos planteados (p. 183).

4.2.1.1. Funciones de los sistemas de información

Al igual que cualquier sistema, el de información también posee elementos, una estructura de relaciones y propiedades. La interdependencia entre sus distintos componentes y la relación con su ambiente se encuentran dotadas de características que tomarán como marco un conjunto de funciones distintivas y propias de este sistema. Así, es posible esquematizar a un sistema de información en base a sus actividades y funciones. Siguiendo a Volpentesta (2004), estas funciones son:

Figura 4.4.: Funciones y actividades de los sistemas de información



Fuente: elaboración propia en base a Volpentesta (2004).

1) Recolección de elementos de entrada: esta función conecta al sistema con su entorno dado que a través de ella consigue los elementos de entrada necesarios. En este sistema, estos elementos se denominan datos y representan todos aquellos acontecimientos, operaciones o transacciones que se dan de manera rutinaria y que se caracterizan por su gran caudal. La función de recolección se lleva a cabo a través de dos actividades consistentes en la captación y registro de datos. Ambas actividades se

realizan en base a requerimientos previamente establecidos para preparar estos elementos de entrada de forma que puedan ser utilizados y almacenados.

2) Almacenamiento de datos: representa una de las funciones esenciales ya que gracias a ella será posible la creación y mantenimiento de archivos que constituirán una gran base de datos que, unida al conocimiento, permitirá generar procesos de aprendizaje y adaptación. Esta función se encuentra conformada por tres actividades: archivo de datos, clasificación y recuperación.

   Los datos que se recolectan deben sistematizarse a fin de que resulten utilizables cada vez que se lo requiera, pero también deben ser resguardados y protegidos de pérdidas o accidentes. El archivo de datos es la actividad encargada de velar por estos elementos y constituye una barrera de acceso que impedirá su consulta o modificación por quienes no se encuentran autorizados. Este acceso no debe ser indiscriminado, pero sí debe resultar fácil para quienes deben trabajar en ellos. Para su utilización, los datos deben ser identificados a través de campos que podrán estar asociados a nombres, símbolos o valores. A través de estos campos será posible establecer interrelaciones que permitirán conformar un registro que, al interrelacionarse con otros registros, darán como resultado un archivo. La red conformada por un conjunto de archivos dará origen a una base de datos.

   Cada vez que se realice el registro de una transacción, la misma debe estar asociada a una clasificación basada en uno o varios atributos a fin de que sea posible su agrupación o disposición en base a un orden o secuencia particular. La cantidad de atributos o características que se tomen en cuenta para la sistematización no debe ser tan escasa como para imposibilitar la obtención de la información que se necesite ni tan amplia como para aumentar de manera indiscriminada la base de datos.

   La recuperación consiste en facilitar el acceso a todo dato que se encuentra dentro de la base y que depende de una clasificación previamente realizada. Esta actividad debe permitir que el acceso se realice en el menor tiempo posible, en especial cuando se requiere la recuperación en tiempo real (mismo momento en que la transacción tiene lugar). La recuperación puede realizarse a través de consultas específicas que permitan traer datos primarios, procesando nuevamente los mismos para dar respuestas a demandas determinadas en momentos determinados o bien, a través de la interacción con modelos donde el usuario pueda obtener respuesta frente a los distintos escenarios con los que necesite trabajar.

3) Procesamiento de datos en información: al igual que cualquier sistema, el de información está conformado por procesos que se encargan de la transformación de los elementos de entradas (datos) en salidas (información). Estos procesos pueden consistir en tareas de clasificación, cálculos, análisis, organización, relación y en cualquiera otra actividad o conjunto de actividades que conlleven la manipulación de datos a fin de transformarlos en respuesta a las necesidades de información de los diversos usuarios.

4) Salida de productos de información: las salidas de información (elementos de entrada procesados) pueden ser mensajes, documentos o informes, cualquiera sea su formato y soporte, y deben estar orientadas a expresar información referida a actividades pasadas, a estados actuales o a proyecciones futuras, a señalar acontecimientos importantes, oportunidades, problemas, amenazas o a iniciar o confirmar acciones. Con dicho propósito esta función realizará tres actividades: compresión, transmisión y exposición de datos.

   Dado el gran volumen de datos que es posible encontrar dentro del dominio de una organización, la compresión, a través de la filtración y la condensación, buscará reducir el contenido de la información, pero dotándola de valor al otorgarle claridad. A fin de que las salidas cumplan con su razón de ser, la información producida debe ser comunicada y transmitida. Esta transmisión se genera frente a dos circunstancias: porque la información se encuentra centralizada y requiere ser conocida por otros sectores o niveles particulares o porque es necesario reunir la información que se encuentra descentralizada. Dentro de esta actividad, los recursos de comunicación juegan un papel de vital importancia ya que solo cuando la información es comunicada es posible generar conocimiento y lograr así ventajas competitivas. Por último, a través de la exposición mediante mensajes, documentos, informes periódicos, estandarizados, a medida, de datos críticos, entre otros, es posible dotar de utilidad a la información para los usuarios. Esta aclaración merece importancia dado que, no toda la información que es producida por el sistema es expuesta, sino que puede estar reservada para operar dentro del propio sistema.

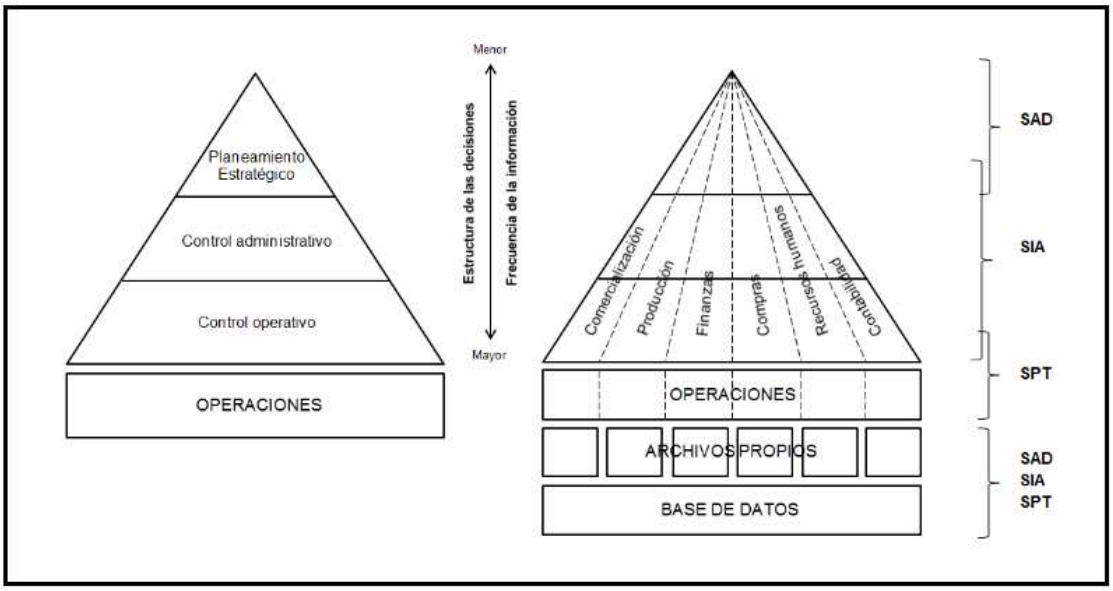
5) Control del desempeño del sistema: una de las propiedades de los sistemas en general lo constituye la retroalimentación de forma que todo sistema contiende un proceso de supervisión o evaluación encargado de mantener su funcionamiento eficiente y teniendo en cuenta sus objetivos. El sistema de información no solo debe generar información para su exterior sino también para su propia operatoria de forma que la misma puede

estar orientada al control las actividades relacionadas con los elementos de entrada, a los procesos, a los elementos de salida y a las actividades de almacenamiento.

4.2.1.2. Estructura de los sistemas de información

El objetivo principal de los sistemas de información consiste en generar toda aquella información necesaria no solo para los usuarios externos sino también para satisfacer los procesos administrativos y las actividades que se desarrollan internamente. De esta forma encontramos sistemas diseñados, estructurados y orientados hacia las actividades y a la toma de decisiones y sistemas diseñados, estructurados y orientados hacia sus funciones organizacionales (Volpentesta, 2004).

Figura 4.5.: Estructura de los sistemas de información



Fuente: Sistemas administrativos y sistemas de información (Volpentesta, 2004).

4.2.1.2.1. Orientados a las actividades organizacionales y a la toma de decisiones

Los niveles organizacionales son los encargados de realizar las distintas tareas necesarias para confluir hacia una meta común y para ello necesitan información para la toma de decisiones. Básicamente es posible dividir dichos niveles en tres categorías, las cuales se diferenciarán por sus actividades, por la información que requieren y por las decisiones que deben tomar. Así encontramos al nivel operativo encargado de las actividades y transacciones elementales, donde las decisiones se toman de manera rutinaria y la información es requerida en tiempo real. El nivel administrativo o gerencial realiza tareas de seguimiento comparando lo alcanzado con los objetivos a corto plazo, sus decisiones son tomadas de manera menos frecuente que el nivel operativo por lo que la información

requerida suele ser de menor frecuencia y no siempre respeta requerimientos definidos o establecidos. Por las características de las decisiones de este nivel, puede requerirse información externa e interna que no necesariamente proviene del nivel operativo sino también de aquella que es generada por este mismo nivel. Finalmente, el nivel estratégico suele enfocarse en decisiones a largo plazo y que se encuentran altamente influenciadas por el entorno. Sus decisiones suelen ser de menor frecuencia que en niveles anteriores por lo que las necesidades de información también son menores (Laudon y Laudon, 1996). Estos tres niveles se encuentran apoyados por tres tipos de sistemas que buscarán cubrir sus necesidades informativas y que se fusionarán en una estructura piramidal:

1) Sistema de procesamiento de transacciones (SPT): registra las transacciones diarias y de rutina y que tienen como origen operaciones internas y, principalmente, con el entorno. Dado el abultado volumen de transacciones, se requiere que quien utilice este sistema posea gran conocimiento de ellas, que ejecute los procedimientos de acuerdo a lo establecido permitiendo un manejo uniforme de la totalidad de los datos ingresantes de forma que, al momento en que se lo necesite, puedan ser obtenidos al instante. Aunque representa el primer paso en la obtención de datos provenientes del entorno, este sistema es el responsable de la permanente actualización de los archivos y de las bases de datos generando gran cantidad de salidas de información tanto para uso interno como externo por lo que es considerado el principal generador de información. Este sistema tiene dos propósitos: obtener un registro completo de todas las operaciones o transacciones que han tenido lugar y servir de base para la preparación de informes (Laudon y Laudon, 1996 y Volpentesta, 2004).

2) Sistema de información administrativa (SIA): sirve a las funciones de planeación, control y toma de decisiones a nivel administrativo. En general resumen la información obtenida en los SPT y emplean modelos muy sencillos para la presentación de informes con contenidos específicos y preestablecidos. Como los problemas que se tratan en este nivel se presentan con cierta frecuencia y están destinados a hechos internos más que externos, los requerimientos de información son cubiertos por el nivel anterior y por cualquiera otra que se encuentre en la organización, aunque eventualmente necesitarán o requerirá información del entorno (Laudon y Laudon, 1996 y Volpentesta, 2004).

3) Sistema de apoyo para la toma de decisiones (SAD): sirve al nivel estratégico donde la toma de decisiones se orienta a problemas no estructurados o programados. Están diseñados para incorporar gran cantidad de información externa que, combinada con la generada por los dos sistemas anteriores (predominantemente por el SIA), suplirán

las necesidades informativas. Dado que se encargan de problemas de naturaleza no muy recurrente e incluso única, donde los riesgos de una mala decisión pueden implicar un elevado error, el diseño de este sistema debe poseer gran capacidad para abarcar diversidad de situaciones haciendo que la información sea altamente interactiva. Los requerimientos informativos del nivel estratégico se caracterizan por no siempre ser fácilmente determinables por lo que la adaptabilidad y flexibilidad debe ser mayores que en los sistemas anteriores permitiendo la creación de nueva información analizando lo que ya se posee e incorporando aquello que no y que resulta de gran utilidad. El énfasis puesto en estos sistemas es el apoyo al razonamiento y no la automatización de las decisiones de forma que ayudan al usuario, pero nunca reemplazan su decisión (Laudon y Laudon, 1996 y Volpentesta, 2004).

4.2.1.2.2. Orientados a las funciones organizacionales

Según Volpentesta (2004), una función es una serie de actividades relacionadas en forma cercana que por sus características distintivas hacen que cada una tenga necesidades específicas de información. Un sistema de información está conformado por subsistemas que incluyen recursos, cuando estos son utilizados en una función particular, estamos en presencia de una aplicación de sistemas de información. De esta forma, los sistemas pueden tener aplicaciones en compras, ventas, producción, etc. y conformar subsistemas de apoyo de comercialización, de producción, de finanzas, de compras, de recursos humanos, contabilidad, entre otros. Como consecuencia, el sistema queda conformado como una asociación de sistemas de información orientados al apoyo de las distintas funciones organizacionales y que encontrarán conexión en una base común. Cada uno de estos sistemas funcionales puede contar con archivos de datos propios que se utilizan de forma individual para sus distintas tareas básicas pero que luego se encontrarán conectados a una base común. Cada una de estas aplicaciones requerirá de secciones referidas al procesamiento de transacciones (SPT), a los sistemas de apoyo para la administración (SIA) y para el planeamiento estratégico (SAD).

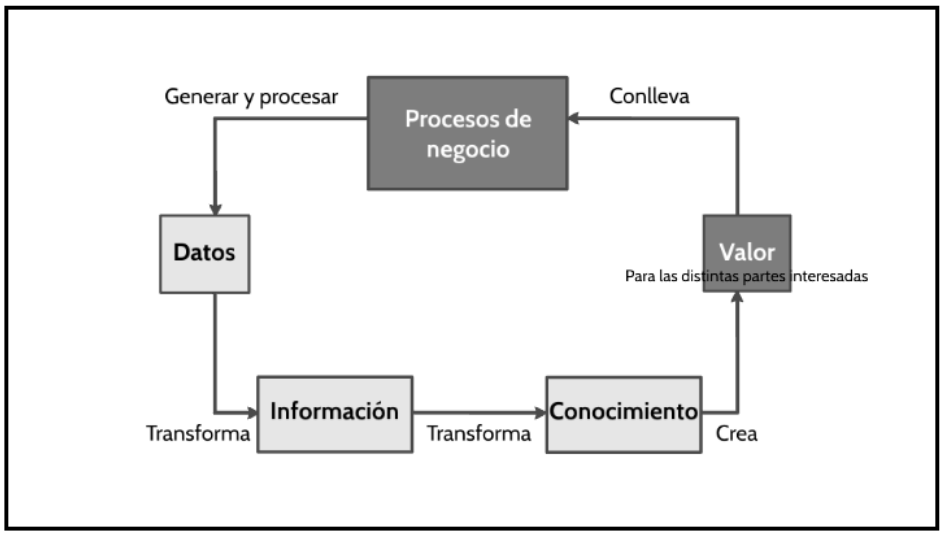
Aunque este esquema funciona perfectamente para la comprensión de un sistema orientado a las funciones, en la actualidad la tendencia consiste en la utilización de procesamientos que integran, como si fuese un solo sistema, varias aplicaciones vinculadas con alguna operatoria común, siendo posible simplificar las interconexiones y eliminando posibles duplicaciones de entradas. De esta forma, se atraviesan los límites funcionales integrando todas o algunas funciones y conformando un sistema capaz de cubrir las necesidades de información de todos los niveles. Independientemente de lo descripto, esto no

necesariamente impide que cada una de las unidades funcionales pueda disponer de archivos o sistemas propios para su uso específico (Volpentesta, 2004).

4.2.1.3. El ciclo de la información

Definidas las funciones y actividades de los sistemas de información y luego de haber logrado obtener una estructura conceptual de los mismos, es posible adentrarnos y comprender el ciclo de la información. Según lo establecido por el IT Governance Institute (2012) en el marco COBIT 5, la información constituye un factor clave que, actuando de manera individual o colectivamente con otros elementos, influye sobre el funcionamiento de algo. Así es posible considerarla como un elemento indispensable que impregna la totalidad la organización y que incluye toda aquella información que es producida y utilizada por esta. Bajo esta concepción, necesita ser gestionada como un recurso dado que es necesaria para mantener a la organización funcionando y bien gobernada pero que, a nivel operativo, también constituye un producto clave en sí mismo siendo posible encontrarla como una etapa dentro de su propio ciclo. Dentro de este, los procesos de negocio generan y procesan datos para transformarlos en información y conocimiento para finalmente generar valor para la organización y sus partes interesadas (IT Governance Institute, 2012).

Figura 4.6.: Ciclo de la información



Fuente: IT Governance Institute (2012).

Cada proceso posee un ciclo de vida, es decir que tiene que ser creado, ejecutado, supervisado y ajustado cada vez que resulte necesario. Dicho de otra manera, cada proceso debe ser diseñado definiendo responsabilidades y la descomposición del mismo en prácticas y actividades, así como sus productos de entrada y salida. Finalmente, en una etapa posterior, el proceso necesita robustecerse y ser crecientemente eficiente para elevar

de manera continua su capacidad. Según el marco mencionado, el ciclo de la información se encuentra asociado a cuatro dimensiones que completan el modelo y que forman parte del proceso total de información (IT Governance Institute, 2012):

- Partes interesadas: son quienes poseen diversos intereses en la información y en función de quienes se fijarán las bases sobre la cuales esta será preparada. Las mismas pueden ser internas o externas y más allá de su individualización, resulta importante identificar sus intereses y el motivo por el cuál poseen esos intereses. Estos intereses se encontrarán relacionados con las metas de la información.

- Metas de la información: se refieren a las dimensiones de calidad de la información, las cuales se encuentran divididas en calidad intrínseca, calidad contextual y de representatividad y, accesibilidad y seguridad (este tema será tratado en el capítulo siguiente).

- Ciclo de vida: está relacionado con las distintas fases del proceso de generación de la información e involucra a los responsables de su creación, de su almacenamiento y mantenimiento y de su utilización:

    a) Planificar: en esta fase se identifican los distintos objetivos, se organiza la estructura y arquitectura de la información y se desarrollan los diversos estándares y definiciones necesarios.
    b) Diseñar.
    c) Construir, adquirir, crear, implementar: consiste en la creación de registros de datos y en la incorporación y carga de archivos.
    d) Usar, operar: está relacionado con las actividades de almacenamiento de la información cualquiera sea su formato (retenida electrónicamente o impresa), de distribución a fin de que encuentre a disposición de las partes interesadas y de utilización cuando se la aplica para los distintos objetivos, así como con las actividades de recuperación y conversión de una forma a otra.
    e) Evaluar o supervisar: asegurar que el proceso funciona correctamente a fin de incorporar valor y de mantener las bases actualizadas, así como otras actividades relacionadas con la gestión de información (mejora, limpieza, fusión, eliminación de datos duplicados, entre otros).
    f) Eliminar o archivar: puede consistir en la destrucción de la información cuando la misma ya no es de utilidad o bien en su archivo permanente.

- Mejores prácticas: está relacionado con todo aquello que tienda a optimizar su soporte físico y portabilidad, accesos e interfaces, lenguaje y formato, tipo, vigencia y significado, nivel de agregación o desagregación, estado, retención, entre otros.

4.2.1.4. Sistemas de información y la tecnología

Los sistemas de información existen más allá de la existencia de la tecnología, aunque en la actualidad resulte difícil separarlos. Dado el recurrente incremento de las actividades organizacionales y del cambiante entorno global, la tecnología ha sabido ser una herramienta de gran utilidad que ha servido con creces a las necesidades de automatización, mecanización y reducción de costos. Aunque es creciente el número de organizaciones que reconocen los beneficios de la tecnología, el éxito en su implementación requiere de una buena administración, de la comprensión del sistema de información en el cual se encontrará inmersa y de una correcta alineación con la cultura, valores y objetivos particulares de cada organización dado que por sí misma es incapaz de generar valor (Serrano González y Zapata Lluch, 2003).

Como ha quedado expresado, la herramienta principal para el logro de ventajas competitivas se encuentra en la información y consecuentemente en el sistema que se utiliza para producirla, utilizarla y resguardarla. La tecnología juega un papel relevante otorgando una característica distintiva a dicho sistema dado que introduce nuevos elementos y abre paso, de manera recurrente, a nuevas formas de captación de datos, de procesamiento, de almacenamiento y de comunicación siendo la rapidez y la agilidad una de sus ventajas principales (Canetti, 2007). Así, considerando las TI, es posible distinguir los siguientes recursos de un sistema de información (Laudon y Laudon, 1996 y Volpentesta, 2004):

1) Recursos de *hardware*: se refiere a los dispositivos electrónicos y electromecánicos que procesan datos y abarcan no solo a las computadoras o equipos físicos sino también a todos los medios tangibles donde ellos son grabados (unidades de procesamiento, alimentación, almacenamiento, salidas).

2) Recursos de *software*: los equipos y recursos hardware se coordinan y controlan a través de programas que constituyen un conjunto de instrucciones, procedimientos, lenguaje y órdenes detalladas que permiten controlar las operaciones del sistema. El software puede ser de dos tipos: software de sistema, que controla y respalda las operaciones del sistema operativo o software de aplicación, que son aquellos programas que dirigen el procesamiento para un uso particular.

3) Recursos humanos: son los usuarios del sistema de información pudiendo ser directos o indirectos según la participación que tengan en el mismo. Serán directos cuando se encuentren encargados de interactuar con el sistema ingresando datos e instrucciones o recibiendo salidas e indirectos cuando aprovechan los informes que este produce, pero no tienen ningún tipo de interacción directa.

4) Recursos de datos: se refieren a las bases de datos y a las bases de conocimiento. Las bases de datos constituyen un conjunto integrado de datos procesados, organizados y almacenados en diferentes tipos de registros. Estas bases permiten la integración de las diferentes áreas o funciones de una organización permitiendo que todos los archivos se agrupen de manera coordinada y unificada. Por su parte, las bases de conocimiento incluyen el aprendizaje sobre diversas circunstancias, reglas y ejemplificaciones consideradas como mejores prácticas.

5) Recursos de redes: están conformados por dispositivos tangibles e intangibles que enlazan las distintas piezas del hardware y constituyen un componente fundamental en el diseño del sistema dado que están destinados a comunicar y transferir la información de un lugar a otro.

En la actualidad, las organizaciones incorporan nuevas tecnologías como componentes fundamentales de sus sistemas de información, aunque muchas veces como una finalidad en sí misma y no como un medio para que el sistema cumpla con su propósito. Confiar en que la tecnología ayudará a la gestión de información por el solo hecho de poseerla implica reducir a estos sistemas a simples conglomerados de dispositivos de avanzada, olvidándonos de uno de sus componentes vitales: el factor humano. Sin embargo, los beneficios y ventajas en el mundo de la información resultan indiscutibles: mayor información, a menor costo y en menor tiempo. Como consecuencia de la inmediatez y la posibilidad de incrementar en gran cantidad los datos a disponer, se incita a una producción desmesurada de información que en muchos casos resulta irrelevante y no muchas veces verificable o susceptible de ser examinada, comparada o profundizada. Surge así la sobrecarga informativa (Sinay, 2017).

Cuando la cantidad de información que circula en una organización sobrepasa la posibilidad de ser absorbida y asumida por parte de los usuarios, estos la reciben y la retransmiten sin procesarla ni reflexionarla de forma que la misma deja de ser aplicable. Como consecuencia, deja de ser un medio para convertirse en un fin importando más su cantidad que su calidad y priorizando el todo sobre más que lo relevante sobre (Sinay, 2017).

Finalmente, es importante aclarar que las nuevas tecnologías, si bien son innovadoras e introducen cambios importantes, aún no han abierto nuevos horizontes dado que significan avances sobre lo ya existente, pero sin alterar demasiado lo esencial de las necesidades a cubrir. Por más que la tecnología ha evolucionado el mundo de la información haciendo que un conjunto de datos resulte más fácilmente manipulable, almacenable y transmisible, estos pueden transformarse en algo que no aporte valor, que no sea presentado en el momento oportuno o bajo los formatos deseables, provocando que los usuarios les asignan menor utilidad y lo perciban como de menor calidad. Frente a ello, y antes de pensar en la tecnología como la única herramienta, aún continuará siendo necesario que cada organización defina qué información necesita, cuándo la necesita, en qué formato, de qué fuentes y cómo esta y el conocimiento que de ella deviene, serán aplicados a sus tareas y a lo largo de toda su infraestructura (Sinay, 2017 y Volpentesta, 2004).

4.3. La calidad y la información

Buscar que un determinado producto reúna los atributos de calidad que el cliente desea para la satisfacción de sus necesidades, ha existido desde épocas artesanales cuando la calidad de un producto se establecía a través de una relación directa entre el artesano y el cliente y donde esta relación permitía la verificación de las características solicitadas en el mismo momento en que el producto era entregado (Gutiérrez Pulido, 2010). Con la llegada de la era industrial aparece la producción masiva y con ella el desvanecimiento del contacto directo entre el fabricante y su cliente surgiendo así la necesidad de introducir procedimientos orientados a alcanzar dicha calidad y dando origen a una nueva figura encargada de evaluarla y detectar los errores susceptibles de interferir en su logro. Esta nueva figura, representada en inspectores, comenzó a ajustarse a determinados estándares fijados por diversas y emergentes normativas que permitieron, a niveles generales, satisfacer las necesidades crecientes y cada vez más exigentes (Gutiérrez Pulido, 2010). Este mismo fenómeno se evidenció con la información y la llegada de las TI.

En las empresas de bienes y servicios, la calidad constituye un concepto bastante claro y palpable pero el problema aparece cuando esta definición debe ser aplicada a la información dado que no existe un consenso único y definido de lo que significa calidad informativa. Una de las principales consecuencias devenidas de la incorporación de tecnología en las organizaciones está asociada con la cantidad de información que sus sistemas son capaces de producir y almacenar. Masividad de datos, agilidad en su manipulación, novedosos métodos de transmisión y diversidad de modelos de exposición de información están relacionados con dichas consecuencias, aunque, por sí solo, el factor cuantitativo no resulta suficiente. Los beneficios de contar con información no están únicamente representados por

la cantidad que es posible poseer sino también por la utilidad que en ella puede encontrarse. Decir que la cuestión no radica en la abundancia o escasez de la información, sino más bien en si la misma recibe el tratamiento adecuado para reflejar fielmente a una organización, consiste en entender que la información solo tiene sentido cuando es susceptible de ser utilizada por alguien y para algo (Coba, 2006).

Desde esta perspectiva, la calidad de la información se encuentra estrechamente ligada a su utilidad y, como consecuencia de la existencia de diversos grupos de interés, se trata de un concepto multidimensional que no se agota en una única definición. En términos generales, puede considerarse que la información es de calidad cuando resulta útil para el usuario y facilita su proceso de toma de decisiones. Representa un concepto complejo, no solo porque constituye una variable no observable de manera directa sino porque se encuentra definida a través de una serie de características que se conciben como partes de una totalidad y sin las cuales, la existencia de la calidad, no sería posible (Huguet Benavent, 2014).

Una verdadera transparencia requiere que las organizaciones ofrezcan toda la información necesaria para conocer la situación real en la cual se encuentra inmersa, incrementando así la confianza en la organización y dotando de mayor estabilidad y seguridad a la toma de decisiones. Para ello, la calidad de la información no puede ser medida independientemente de las personas que la usan, aunque también debe estar diseñada y dirigida a sus productores y a la organización en general, de forma que los elementos o características que componen la calidad no solo deben encontrarse en el producto final (información) sino también en todo su proceso de producción envolviendo tanto a los profesionales auditores como a toda la organización (Huguet Benavent, 2014).

Si bien ha sido notable el avance en el proceso de generación de información gracias a los constantes perfeccionamientos de los métodos de recolección, procesamiento, almacenamiento y comunicación de la información, el eje del problema continúa estando en cómo interpretar las necesidades de información de los usuarios a fin de que los sistemas de información se diseñen y estructuren de forma que permitan dar respuesta a dichas necesidades pero velando siempre por mantener la integridad de los datos y asegurando un grado razonable de confiabilidad en las fuentes de origen, en los procesos, en el archivo y en la transferencia y distribución de las salidas. Dicho de otro modo, la calidad de la información depende en gran parte de la confiabilidad de los datos de los que surge, de los procesos que la generan y de los modelos que se utilizan para exteriorizarla siendo de este modo, la eficiencia y la seguridad de los sistemas el aspecto clave para asegurar la utilidad de la información. Frente a lo expuesto, resulta viable considerar a la calidad de la información como una medida de control a través del análisis de la correspondencia de la

realidad con lo que el sistema de información pretende representar (Rodríguez de Ramírez, 2004 y Canetti, 2007).

Al concebir la calidad de la información desde la perspectiva del usuario y en asociación a sus necesidades, esta representa un concepto relativo que no encuentra una definición única en sí misma sino más bien en la aptitud para su uso. Así, es posible entender a esta calidad como lo mejor de acuerdo con determinadas condiciones, requerimientos, necesidades y expectativas. Si bien no existe una regla genérica que pueda aplicarse a fines definitorios para determinar si algo es o no de utilidad, sí existe un consenso generalizado en considerar que un producto o servicio es de calidad cuando posee la aptitud para ser utilizado en la satisfacción de una necesidad. Así, siguiendo a Camisón, Cruz y González (2006) y teniendo en cuenta diversas normativas existentes al respecto, mencionamos algunas de las definiciones de calidad más representativas:

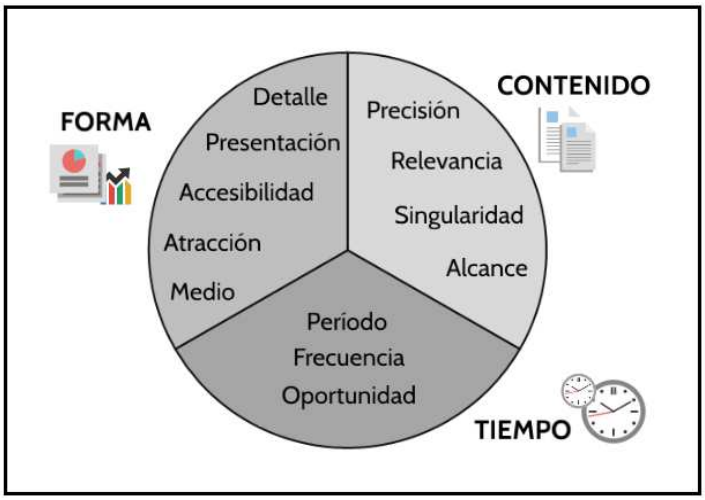
- El British Standards Institute (BSI) entiende por calidad a "la totalidad de rasgos y características de un producto o servicio que tienen que ver con su aptitud para satisfacer una necesidad dada" (p. 163).
- La norma ISO 8402 (complemento de la serie ISO 9000) define a la calidad como "la totalidad de las propiedades y características de un producto o servicio que le confieren la aptitud para satisfacer las necesidades explícitas o implícitas" (p. 163).
- El Japanese Industrial Standards (JIS) define la calidad como "la totalidad de las características o rendimientos propios que son objeto de evaluación para determinar si un producto satisface o no las finalidades de su uso" (p. 163).
- La norma ISO 9000 define la calidad como "el grado en el que un conjunto de características inherentes cumple con los requisitos. En este caso el adjetivo inherente expresa aquí que existe en algo especialmente como una característica permanente" (p. 163).

Siguiendo estas definiciones, es posible asociar a la calidad con un conjunto y totalidad de propiedades y características que se espera que un determinado producto posea para satisfacer una necesidad. Retomando lo desarrollado en apartados anteriores, estas propiedades y características estructurales o funcionales se denominan atributos y pueden referirse a características cuantitativas cuando se centran en cantidades, grados, medidas, entre otros o cualitativas cuando están referidas a cualidades, especies, formas, etc. Las características cualitativas suelen estar dotadas de cierto grado de subjetividad razón por la cual resultan más difíciles de medir que las cuantitativas, pero son las que presentan mayor preponderancia y representatividad al hablar de información (Volpentesta, 2004).

4.3.1. Dimensiones y características de la información

Como ha quedado expresado, la calidad de la información puede ser concebida en base a la utilidad que el usuario encuentra en ella para satisfacer la necesidad que le ha dado origen. Para tener un parámetro que permita evaluar dicha valía resulta necesario recurrir a las características de la información como ponderadores de dicha utilidad en función de cada actividad o decisión particular. De esta forma, es la satisfacción de determinadas cualidades, tanto a nivel general como en distintos grados dependiendo de las necesidades particulares de los usuarios, lo que permitirá juzgar a la información como útil y consecuentemente de calidad. Según la bibliografía consultada, es posible evidenciar tres dimensiones que caracterizan a la información siendo estas el tiempo, el contenido y la forma (Volpentesta, 2004).

Figura 4.7.: Dimensiones y características de la información



Fuente: elaboración propia en base a Volpentesta (2004).

La primera dimisión está relacionada con el tiempo y se encuentra constituida por la oportunidad, el período y la frecuencia. La oportunidad consiste en la posibilidad de disponer de la información en el momento en que se la necesita y con la actualización pertinente. Si bien tiene que ver con poner a disposición de los usuarios toda la información que necesitan dentro de un plazo adecuado, también constituye una característica específica para cada situación particular siendo un atributo clave para determinar su utilidad y calidad. El período, por su parte, se relaciona con la orientación temporal de la información siendo posible que se refiera a situaciones pasadas cuando la misma es histórica, a situaciones presentes cuando es a tiempo real o a situaciones futuras cuando es predictiva. Finalmente, la frecuencia tiene que ver con la cantidad de veces que se solicita, se busca o se prepara esa información. Este tipo de característica se relaciona con una de las funciones básicas de los sistemas de información dado que se verá reflejada en la elaboración de informes que

servirán a los distintos niveles organizativos e incluso a terceros o usuarios externos (Volpentesta, 2004).

En cuanto al contenido, las características distintivas son la relevancia, la precisión, el alcance y la singularidad. La primera de ellas se refiere a la importancia que adquiere la información en función de su aplicabilidad a una determinada situación y en relación a una acción o decisión en particular. La relevancia implica que la información necesaria para una situación concreta y específica debe: a) estar vinculada con las necesidades del usuario que la solicita (pertinencia), b) ser lo más completa posible (integridad) y c) proporcionar solo lo que es requerido (brevedad). La precisión consiste en que la información debe encontrarse libre de errores y de tendencias o desviaciones que busquen sesgarla. Aunque es muy difícil hablar de una exactitud del 100% en la información, existe un nivel adecuado de precisión para cada nivel de actividad o proceso decisorio. Esta característica siempre debe evaluarse conjuntamente con la relación costo-beneficio de la información dado que, generalmente, a mayor precisión, mayor será el costo de la misma. Por otro lado, el alcance está relacionado con el uso que se le da a la información. Cuando la misma está dirigida a la totalidad de una organización, su alcance será amplio, pero cuando se utilice para una actividad en particular y puntual, el alcance será preciso y definido. La singularidad, relacionada con el punto anterior, determina la diferencia de valor que existe entre diversos elementos informativos. Así, la información que tiene libre circulación y que es compartida sin restricciones tendrá menos valor que aquella cuya circulación o acceso se encuentra restringido. Por esta razón la información creada internamente por una organización puede estar dotada de un mayor valor, de una mejor custodia y encontrarse disponible solo para determinados niveles o personas (Volpentesta, 2004).

Por último, la dimensión forma alberga cinco características: presentación, detalle, medio, atracción y accesibilidad. La presentación consiste en la manera en que se estructura y se expone la información dependiendo de si la misma es cuantitativa o cualitativa. El detalle se refiere al grado de apertura, es decir si se presenta la totalidad de los elementos o un resumen a través del agrupamiento. El medio hace referencia al soporte en el cual se presenta la información pudiendo ser impreso, visual o auditivo. La atracción, se refiere a que la información, independientemente de su utilidad o valor, debe llamar la atención del potencial usuario en especial si se considera la sobreabundancia informativa y puede estar relacionada con la forma de presentación, al formato o al medio utilizado. Finalmente, la accesibilidad se refiere, por un lado, a la dificultad o tiempo requerido para la obtención de la información y, por otro, a la manera en que se encuentra estructurada a fin de que pueda ser entendida y recuperarse de lo que de ella se necesite sin lidiar de manera recurrente con gran cantidad de datos (Volpentesta, 2004).

Dada la diversidad de características cualitativas que existen y las distintas definiciones y agrupaciones, es posible encontrar otra categoría de dimensiones sobre las cuales se puede construir dicha calidad y que merece ser expuesta dada su diferente perspectiva. Al respecto, González Valiente (2014) expone cuatro dimensiones que pueden ser consideradas como determinantes de calidad, así como las distintas características cualitativas que quedan enmarcadas dentro de ellas. De esta forma encontramos a la dimensión intrínseca que concibe a la información como algo que tiene calidad por sí misma, a la dimensión contextual que establece que los requerimientos de calidad se dan en un contexto determinado y a la dimensión representacional y de acceso que enfatizan la importancia de los sistemas apoyados por la tecnología para la accesibilidad de la información y su almacenamiento. Dado que muchas de ellas serán tratadas en el apartado siguiente, las expondremos solo a modo informativo.

Tabla 4.1.: Dimensiones y características de la información

Intrínseca	Contextual	Representacional	Acceso
Precisión	Pertinencia	Entendible	Accesibilidad
Credibilidad	Valor agregado	Interpretabilidad	Facilidad de operación
Reputación	Oportunidad	Razonabilidad	Seguridad
Objetividad	Cantidad apropiada	Sintaxis	Disponibilidad
Realidad factual	Confiabilidad	Control de versiones	Restricción (privilegios)
Integridad	Relevancia	Claridad	Usabilidad
Coherencia	Suficiencia	Originalidad	Localización
Exactitud	Vigencia	Comparabilidad	
Fiabilidad		Compatibilidad	
Libertad de prejuicios		Significatividad	
Consistencia			
Libertad de ambigüedades			
Veracidad			

Fuente: elaboración propia en base a González Valiente (2014).

4.3.2. Partes interesadas y las necesidades de información

Las organizaciones poseen muchas partes interesadas que se encuentran representadas por personas que poseen distintas responsabilidades, expectativas o cualquier otro interés en o dentro de la misma. Estas partes interesadas pueden ser divididas en partes o usuarios internos o externos siendo posible encontrar a los propietarios, accionistas, empleados, proveedores, consumidores, clientes, entes reguladores o el público en general.

Las partes interesadas internas (gobierno, gerencia, empleados, entre otros) son aquellas que interactúan con los diversos sistemas de la organización ingresando datos o recibiendo salidas. Necesitan información constante para la toma decisiones dentro de la empresa y conforman la parte activa en la generación de información. Por su parte, las partes externas (clientes, socios, accionistas, reguladores, público en general) son quienes aprovechan las

salidas de esos sistemas, pero no tienen ninguna interacción con ellos. Necesitan información periódica para tomar decisiones sobre la organización siendo receptores pasivos de la misma (Lardent, 2001).

Cada una de estas partes poseen diversos roles y a fin de poder cumplirlos, requieren información. Sus decisiones, actividades y responsabilidades harán que sus necesidades y expectativas de información sean diferentes y muchas veces contradictorias entre sí por lo que constituye una responsabilidad de la propia organización crear información de valor a fin de cubrir la mayor cantidad de esos requerimientos (IT Governance Institute, 2012). Este análisis de necesidades demanda procesos sistemáticos y planificados orientados a determinar los distintos requerimientos de información y los diversos hábitos de quienes la utilizan con la finalidad de proporcionar productos o servicios de información dirigidos a satisfacer las necesidades de cada grupo de interés, generar confianza en la organización y lograr altos niveles de uso de estos productos o servicios de información (Soy i Aumatell, 2003).

Figura 4.8.: Satisfacción de las partes interesadas

Fuente: elaboración propia.

4.3.2.1. Partes interesadas internas

Como ha quedado expresado, la información constituye un elemento indispensable que impregna la totalidad de una organización incluyendo no solo la información producida por esta sino también la utilizada, pudiendo ser información proveniente de la propia organización o de fuentes externas. Cualquiera sea su fuente u origen, todas son necesarias para mantener a la organización funcionando y bien gobernada, sin embargo, a nivel operativo la información constituye un producto clave en sí mismo (IT Governance Institute, 2012).

El usuario interno es toda aquella persona que forma parte de la organización y que necesita de documentos, información y procedimientos como materia prima para poder adicionarle su

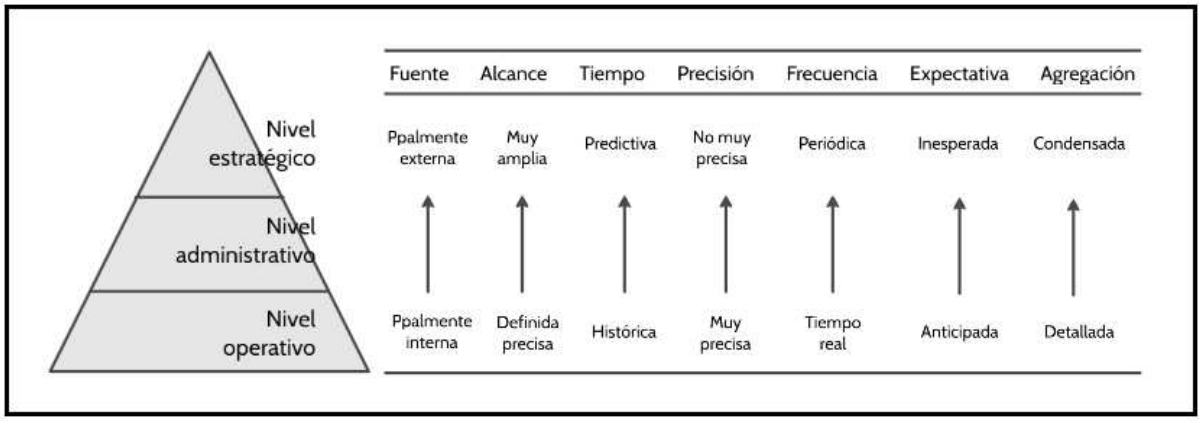
propio trabajo y generar otro tipo de salidas que a su vez pueden constituir entradas para otros usuarios internos e incluso, externos. Dentro de una organización, todos los miembros son clientes y proveedores de otros miembros pudiendo verificarse una cadena de suministros donde la salida de un proceso se convierte en la entrada de otro y la salida de este último en la entrada de un proceso para un externo. En esta cadena, cada proceso entrega un producto con valor intrínseco (Camisón et al., 2006).

Enfocándonos en estos usuarios internos y siguiendo la estructura organizativa dividida en niveles (estratégico, administrativo y operativo), es posible advertir que existe una marcada diferencia y contraste entre las características de la información que cada uno de estos niveles necesita, ya que sus necesidades se encuentran altamente influenciadas y relacionadas con los distintos tipos de decisiones que cada uno de ellos debe abordar. Así, en los niveles operativos, las situaciones que se presentan se dan de manera repetitiva y rutinaria de forma que las consecuencias de las decisiones a tomar se conocen de manera certera. La naturaleza repetitiva y la marcada precisión que requiere la información hacen posible que las decisiones a tomar se encuentren completamente definidas y en algunos casos, incluso, automatizadas a través de procedimientos anticipados. La información que se requiere debe estar dotada de una mayor frecuencia y los niveles de detalle suelen ser mucho más amplios que en los rangos más elevados. Ejemplo de ello lo constituye la decisión de adquisición de materia prima para continuar con un determinado nivel de producción siendo necesario contar con información detallada de la cantidad de insumos en stock y los necesarios a adquirir, así como determinadas características cualitativas que los mismos deben reunir. Este tipo de decisiones requiere de información principalmente interna, precisa y detallada como la cantidad de producción o cantidad y tipo de insumos en stock a fin de anticiparse a la posibilidad de correr con faltantes (Volpentesta, 2004).

Por otro lado, en los niveles más altos, las decisiones que deben tomarse son de tipo no programadas donde el uso de fuentes externas de información es generalmente mayor que en los otros niveles. Las situaciones que requieren atención en estos rangos tienen que ver con situaciones que se presentan con una frecuencia muy baja e incluso por una única vez, donde no es posible establecer reglas concretas y que no suelen tener soluciones previas ni procedimientos anticipados. Ejemplo de ello constituye la adquisición de una nueva planta o la apertura de sucursales. Ambos tipos de decisiones enunciadas en este y el anterior párrafo representan extremos, por lo que es posible ubicar al nivel administrativo dentro de estos dos niveles, aunque las características que se soliciten de la información variarán según las decisiones (Volpentesta, 2004).

A modo de ejemplo se tomarán algunas de las propiedades o atributos explicados con anterioridad a fin de observar, de manera clara, como los mismos cambian a medida que se asciende o desciende de nivel quedando clara la marcada diferencia que puede existir entre las distintas partes interesadas internas. Lo cierto es que, independientemente de lo que cada actor o parte requiera, los sistemas de información deben ser susceptibles de generar la información que satisfaga a cada uno de ellos permitiéndoles cumplir con su rol o responsabilidad determinada.

Figura 4.9.: Características de la información y los niveles organizacionales



Fuente: Sistemas administrativos y sistemas de información (Volpentesta, 2004).

Cada gobierno u organización en particular puede fijar requisitos diferentes o adicionales en función de sus propios intereses. Sin embargo, esos requisitos no deben afectar o interferir en la elaboración de información destinadas a terceros y que se encuentra expuesta a través de estados contables o financieros.

4.3.2.2. Partes interesadas externas

Dado el gran abanico de personas externas interesadas en las organizaciones, es dable pensar que muchos de esos intereses puedan presentar contradicciones y como consecuencia, la información requerida para suplir esas diversas necesidades deba ajustarse a determinados estándares y normativas que buscan garantizar su fiabilidad. Cuando la información se encuentra destinada a terceros, su proceso de generación debe desarrollarse siguiendo las normas contables generalmente aceptadas dando origen a los estados contables o estados financieros según el marco de cumplimiento determinado. Estos estados son considerados una importante fuente de información para los agentes económicos dado que permiten reducir la incertidumbre que todo proceso decisorio trae aparejado. En este sentido, el objetivo de la contabilidad también consiste es proporcionar información útil para la toma de decisiones (Huguet Benavent, 2014).

La contabilidad o el sistema de información contable es un sistema que se desprende del sistema de información y una de sus funciones principales consiste en la elaboración de informes especiales con determinada frecuencia y siguiendo un conjunto de requerimientos legales y comerciales de información destinada a terceros. Siguiendo a Volpentesta (2004), el sistema contable forma parte de los SPT dada su función de procesamiento de datos de las transacciones que afectan patrimonialmente a la organización y de generación de gran parte de los datos que luego se utilizaran en otras aplicaciones. A su vez, y continuando con la línea desarrollada en el capítulo anterior, es posible definir al sistema de información contable como aquel que comprende las personas, los métodos, los procedimientos y los recursos utilizados por la entidad para llevar un control de sus actividades y presentarla en forma útil para la toma de decisiones. Su rol consiste en desarrollar y comunicar la información necesaria para planear y evaluar el cumplimiento de los objetivos siendo sus elementos los registros contables, los métodos y medios de registración, los planes y manuales de cuentas, el archivo de documentación, controles, informes a emitir, entre otros (Canetti, 2007).

La emisión de informes destinados a terceros, así como la generación de toda la información que los mismos contienen, deben desarrollarse en base a una serie de principios contables generalmente aceptados contenidos en marcos de cumplimiento emitidos y respaldados por un organismo regulador. Estas normas, al tener en cuenta la diversidad de propósitos, objetivos y necesidades, moldean la información a ser presentada a fin de satisfacer, en la medida de lo posible, al gran abanico de usuarios.

Tabla 4.2.: Los atributos de la información y los marcos de cumplimiento

Marco conceptual RT 16 **Requisitos de la información contenida en estados contables**	**Marco conceptual NIIF** **Características cualitativas de la informacion financiera**
	Características cualitativas fundamentales
1) Pertinencia o atingencia. **2)** Confiabilidad o credibilidad. **a)** Aproximación a la realidad. **-** Esencialidad o sustancia sobre forma. **-** Neutralidad, objetividad o ausencia de sesgos. **-** Integridad. **b)** Verificabilidad. **3)** Sistematicidad. **4)** Comparabilidad. **5)** Claridad o comprensibilidad.	**1)** Relevancia. **2)** Representación fiel. **a)** Completa. **b)** Neutral. **c)** Libre de error. **Características cualitativas de mejora** **1)** Comparabilidad. **2)** Verficabilidad. **3)** Oportunidad. **4)** Comprensibilidad.
Restricciones que condicionan el logro de los requisitos	**Restricciones que condicionan el logro de los requisitos**
1) Oportunidad. **2)** Equilibrio entre costos y beneficios. **3)** Impracticabilidad.	**1)** Equilibrio entre costos y beneficios.

Fuente: elaboración propia en base a FACPCE (2000) y IASB (2010).

En nuestro país, este marco normativo está constituido por las Normas Profesionales Argentinas Contables, de Auditoría y Sindicatura emitidas por la Federación Argentina de Consejos Profesionales de Ciencias Económicas (FACPCE). Dichas normas, en su Resolución Técnica número 16 Marco Conceptual de Normas Contables Profesionales (FACPCE, 2000), establecen que, a fin de cumplir con su finalidad, la información destinada a terceros, debe reunir los siguientes requisitos que deben ser considerados en conjunto y buscando un equilibrio entre ellos mediante la aplicación del criterio profesional:

a) Pertinencia o atingencia: la información debe ser apta para satisfacer las necesidades de los usuarios. En general se considera que esto ocurre cuando la información tiene valor confirmatorio al permitir la confirmación o corrección de evaluaciones realizadas previamente o bien cuando tiene valor predictivo al ayudar a los usuarios a aumentar la probabilidad de pronosticar correctamente las consecuencias de los hechos pasados o presentes.

b) Confiabilidad o credibilidad: la información debe ser creíble para los usuarios de forma que estos la empleen en sus distintos procesos decisorios. La información es confiable cuando se aproxima a la realidad y es susceptible de ser verificable:

- Aproximación a la realidad: la información debe guardar una correspondencia razonable con los fenómenos que pretende describir de forma que no debe estar afectada por errores u omisiones importantes ni encontrarse sesgada con el objetivo de beneficiar los intereses particulares del emisor o de algunos usuarios determinados. Aunque la búsqueda de aproximación a la realidad resulte fundamental, es normal que la información contable sea inexacta debido a que algunos hechos u operaciones son muy difíciles de medir o porque involucran incertidumbre sobre hechos futuros. Para que la información se aproxime a la realidad, debe ser esencial, neutral e integra:

    1. Esencialidad o sustancia sobre forma: los hechos y operaciones deben exponerse basándose en su sustancia y realidad económica.
    2. Neutralidad, objetividad o ausencia de sesgos: no debe existir deformaciones que favorezcan al ente emisor o que sean susceptibles de influir de una manera determinada en la conducta de los usuarios a fin de orientar la toma de decisiones hacia una dirección en particular o buscando la obtención de un resultado o desenlace predeterminado. Para velar por la neutralidad, quienes preparan la información deben actuar con objetividad.

3. Integridad: la información debe ser completa. La omisión de información pertinente y significativa puede convertir a la misma en falsa o conducente a error y, por lo tanto, no confiable.

- Verificabilidad: la representatividad de la información contenida en los estados contables debe ser susceptible de comprobación por cualquier persona con pericia suficiente.

c) Sistematicidad: la información suministrada debe encontrarse orgánicamente ordenada en base a lo establecido por las normas contables profesionales.

d) Comparabilidad: la información debe ser susceptible de comparación con información del mismo ente a la misma fecha o período, del mismo ente a otras fechas o períodos y de otros entes siempre que las normas aplicadas sean las mismas. Ello requiere que toda la información esté expresada en la misma unidad de medida, que los criterios para la cuantificación de datos sean coherentes, que cuando los estados contables incluyan información a más de una fecha o período, todos los datos estén preparados sobre las mismas bases (utilización de las mismas reglas, períodos comparados de igual duración, no afectación de dichos períodos por operaciones estacionales o que no existiesen otras circunstancias que afecten las comparaciones).

e) Claridad o comprensibilidad: la información debe prepararse utilizando un lenguaje preciso que evite ambigüedades, que sea inteligible y fácil de comprender para los usuarios interesados y que posean conocimiento razonable de las actividades económicas, del mundo de los negocios y de la terminología aplicable. Sin embargo, este tipo de información no puede excluir aquello que se considera pertinente a las necesidades de los usuarios por el simple hecho de que su complejidad la haga de difícil compresión.

Adicionalmente a las características anteriores, la norma incluye tres atributos más que deben contemplarse en la elaboración de información destinada a terceos, pero cuyo logro puede limitar, en algún grado, el cumplimiento de lo descrito con anterioridad. Así, encontramos lo que la norma menciona como restricciones que condicionan el logro de los requisitos:

f) Oportunidad: la información debe suministrarse en el tiempo conveniente para los usuarios de forma que tenga la posibilidad de influir en la toma de decisiones ya que un retraso indebido puede hacerle perder pertinencia. Es necesario balancear los

beneficios relativos de la presentación oportuna y de la confiablidad de la información teniendo en cuenta cuál es la mejor manera de satisfacer las necesidades de los usuarios. Es importante considerar que hay casos en los que, para que no pierda utilidad, la información sobre una transacción o hecho debe ser presentada antes de que todos sus aspectos sean conocidos deteriorando así su confiablidad. Por otro lado, si la presentación de dicha información se demorase hasta que todos esos aspectos sean conocidos, la misma sería altamente confiable, pero de poca utilidad para quienes debían tomar sus decisiones en un intervalo de tiempo determinado.

g) Equilibrio entre costos y beneficios: los beneficios derivados de la disponibilidad de información deberían exceder a los costos de proporcionarla.

h) Impracticabilidad: la aplicación de una norma o criterio contable será impracticable cuando el ente no pueda aplicarlo tras efectuar todos los esfuerzos razonables para hacerlo.

En consonancia con la normativa nacional, la normativa internacional, a través del Marco Conceptual para la Información Financiera emitido por la International Accounting Standards Board (IASB, 2010), también ha sabido expedirse en el tema definiendo las características cualitativas que debe reunir la información financiera clasificándolas en características fundamentales y de mejora. Según este marco, el objetivo de la información financiera con propósito general es proporcionar información financiera sobre una entidad de forma que satisfaga las necesidades del mayor número de usuarios principales. Para que la información financiera sea útil, debe ser relevante y representar fielmente lo que pretende describir considerando que esta información se verá mejorada en la medida en que sea comparable, verificable, oportuna y comprensible. Al respecto, el IASB (2010) establece:

Para que sea útil, la información debe ser relevante y estar fielmente representada (características cualitativas fundamentales). Ni la representación fiel de un fenómeno irrelevante ni la representación no fidedigna de un fenómeno relevante ayudan a los usuarios a tomar decisiones adecuadas.

a) Relevancia: la información financiera es relevante si es capaz de influir en las decisiones de los usuarios incluso si algunos eligen no aprovecharla o la conocen por otras fuentes. Se dice que la información es susceptible de influir en las decisiones de los usuarios si la misma contiene valor predictivo, valor confirmatorio o ambos, aunque existe consenso en considerar que ambos valores están relacionados. Se considera que la información contiene valor predictivo si puede utilizarse como un dato de entrada en

los procesos empleados por los usuarios para predecir resultados futuros y valor confirmatorio si confirma o cambia evaluaciones anteriores. Sin embargo, si la información tiene valor predictivo, habitualmente también contiene valor confirmatorio. De esta característica cualitativa fundamental surge lo que se conoce como materialidad o importancia relativa. Se dice que la información es material o posee importancia relativa si su omisión o expresión inadecuada puede influir en las decisiones.

b) Representación fiel: para ser útil la información no solo debe representar los fenómenos relevantes, sino que también debe representarlos fielmente. Es importante aclarar que una representación fiel por sí misma, no da necesariamente lugar a información útil. Para ello se requiere de tres características que deben ser maximizadas en la medida de lo posible:

    1. Completa: incluir la totalidad de la información necesaria para que el usuario comprenda el fenómeno que está siendo representado, incorporando todas las descripciones y explicaciones necesarias.
    2. Neutral: no poseer sesgo, ponderación, enfatización, atenuación o manipulación en la selección o presentación de forma que la misma sea percibida como favorable o adversa. La información neutral no significa información sin propósito o influencia, la misma debe influenciar, pero siempre de buena fe.
    3. Libre de error: no existencia de errores u omisiones en la descripción del fenómeno ni en el proceso utilizado para la producción de la información, sin embargo, esto no significa perfectamente exacto en todos los aspectos.

Por otro lado, las características cualitativas de mejora, presuponen la existencia y cumplimiento de las características fundamentales por lo que vienen a mejorar la utilidad de la información relevante y fielmente representada. Deben maximizarse en la medida de lo posible, aunque individualmente o en grupo no pueden hacer que la información sea útil si la misma es irrelevante y/o no representa fielmente la realidad.

c) Comparabilidad: la información es útil si puede ser comparada con información similar sobre otras entidades y con información de la misma entidad, pero en otro período o fecha. Esta característica permite identificar y comprender similitudes y diferencias entre partidas y es posible cuando se observa congruencia en la aplicación de los mismos métodos para las mismas partidas, de período a período o en un mismo período entre distintas entidades. Aunque la comparabilidad no significa uniformidad, es posible conseguir cierto grado de ella satisfaciendo las características fundamentales. La representación fiel de un fenómeno económico relevante debería tener naturalmente

algún grado de comparabilidad con una representación fiel de un fenómeno económico relevante similar de otra entidad. Es importante comprender que, aunque un fenómeno económico único puede ser representado fielmente de múltiples formas, ello puede influir negativamente en su comparabilidad.

d) Verificabilidad: implica que observadores independientes, diferentes y debidamente informados podrían alcanzar un acuerdo, aunque no necesariamente completo, de que una descripción particular es una representación fiel. La información cuantificable no necesita ser una estimación única para ser verificable dado que también puede serlo en un rango posible de importes y de probabilidades relacionadas. La verificación puede ser directa o indirecta ya sea comprobando una representación mediante la observación directa o a través de la comprobación de los datos de entrada, fórmulas o técnicas y recalculo de resultados utilizando la misma metodología.

e) Oportunidad: disposición a tiempo de la información de forma que tenga la capacidad o posibilidad de influir en sus decisiones. Generalmente mientras más antigua es, menor utilidad tiene, aunque puede continuar siendo oportuna cuando se necesite identificar o evaluar tendencias.

f) Comprensibilidad: se logra a través de la clasificación, caracterización y presentación clara y concisa. Aunque algunos fenómenos poseen complejidad por sí mismos y no es posible facilitar su comprensión, su exclusión podría conllevar a informes incompletos y potencialmente engañosos. Es importante aclarar que la información brindada en los informes financieros, se prepara para usuarios que poseen un conocimiento razonable de las actividades económicas y del mundo de los negocios. A veces, incluso estos usuarios diligentes pueden requerir asesoramiento particular para alcanzar la comprensibilidad de fenómenos complejos.

De la misma manera que sucede en la normativa nacional, la internacional también reconoce que pueden existir restricciones que condicionen el logro de los requisitos, pero solo considera al costo como una restricción dominante. Desde esta perspectiva, la preparación de la información financiera impone costos que deben estar justificados por los beneficios que esta trae aparejada. En este punto, se considera que son los usuarios quienes, en última instancia, cargarán con estos costos en forma de rentabilidades reducidas. Por otro lado, si no se proporciona información necesaria, los usuarios podrían incurrir en costos adicionales para obtener esa información en otro lugar o bien para estimarla. Por su parte, la comunidad también podría verse afectada.

4.3.2.3. Características de la información según normativas particulares

Si bien lo tratado hasta el momento se encuentra orientado a las necesidades propias de la información utilizada dentro de las entidades y a normativas de aplicación obligatoria para la emisión de información destinada a terceros, es importante aclarar que existen otras normativas específicas que también sirven de marco para ayudar a las entidades a comprender e incluir dentro de sus procesos de información todos aquellos conceptos y características que hacen de la misma una herramienta útil para los potenciales procesos decisorios.

Específicamente orientados a los contextos tecnológicos y a las tecnológicas de la información y telecomunicaciones encontramos dos marcos ampliamente reconocidos que también brindan una exposición clara y detallada de aquellas cualidades que, aún mediante la influencia de los avances tecnológicos incorporados en los sistemas de información de las organizaciones, merecen una vez más su enunciación ya que la sola incorporación de la tecnología no basta por sí misma para la verificación de su existencia. Así, encontramos al Macro de negocio para el gobierno y la gestión de las tecnologías de la información de la empresa, COBIT 5 y a la norma ISO/IEC 25012, ambas desarrolladas a continuación:

a) COBIT 5: el marco COBIT 5 constituye un marco de trabajo integral que ayuda a las empresas a crear valor desde las tecnologías de la información buscando gobernarlas y gestionarlas desde un punto de vista holístico y considerando los diversos intereses. Este marco ubica a la información y a las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo y consecuentemente procurar su salvaguarda y ser objeto de auditoría (IT Governance Institute, 2012).

   Las empresas tienen muchas partes interesadas y crear valor para ellas significa cosas diferentes y muchas veces contradictorias. Como consecuencia, el órgano de gobierno debe considerar a todas estas partes al tomar decisiones sobre beneficios, evaluación de riesgos y recursos buscando determinar qué es lo que esperan de la información y de las tecnologías relacionadas y cuáles son sus propiedades para asegurarse que el valor esperado sea el realmente proporcionado. A tal fin, realiza una enumeración de los requisitos de la información y los engloba en tres sub-dimensiones de calidad. Para este marco, los requisitos de la información se denominan metas, las cuales representan las declaraciones que describen el resultado deseado o esperado de un proceso (IT Governance Institute, 2012). A continuación se exponen las dimensiones mencionadas y metas de la información contenidas en cada una de ellas.

Tabla 4.3.: Sub-dimensiones de calidad y metas de la información. COBIT 5

Dimensión	Descripción	Metas de la información
Calidad intrínseca	Grado en que los valores de los datos se encuentran en conformidad con los valores reales.	**Precisión:** grado en que la información es correcta y confiable. **Objetividad:** grado en que la información se encuentra libre de prejuicios y es imparcial. **Credibilidad:** grado en que la información es considerada verdadera y creíble. **Reputación:** grado en que la información está altamente considerada en términos de origen y contenido.
Calidad conceptual y de representatividad	Grado en que la información puede ser aplicada por el usuario a sus tareas y grado en que la misma es presentada de manera clara e inteligible, reconociendo que la calidad de la información depende del contexto de su uso.	**Relevancia:** grado en que la información es aplicable y útil para la tarea a realizar. **Completitud:** grado en que la información no tiene carencias y es de suficiente profundidad y amplitud para la tarea . **Vigencia:** grado en que la información se encuentra lo suficientemente actualizada para la tarea a realizar. **Cantidad apropiada de información:** grado en que el volumen de información es adecuado para la tarea. **Representación concisa:** grado en que la información se presenta en forma compacta. **Representación consistente:** grado en que la información se presenta en el mismo formato. **Interpretabilidad:** grado en que la información está expresada en idiomas, símbolos y unidades con definiciones claras. **Comprensibidad:** grado en que la información es fácil de entender. **Facilidad de manipulación:** grado en que la información es fácil de trabajar y aplicar a diversas tareas.
Accesibilidad y seguridad	Grado en que la información está disponible o puede obtenerse.	**Disponibilidad/oportunidad:** grado en que la información está disponible cuando se lo requiera o que sea rápida y fácilmente recuperable. **Acceso restringido:** grado en que la información se restringe para las partes autorizadas.

Fuente: elaboración propia en base a IT Governance Institute (2012).

b) ISO/IEC 25012: Si bien en lo desarrollado hasta el momento se ha hablado de la calidad de la información propiamente dicha, también es posible encontrar normativas destinadas a la calidad de la materia prima de esa información y de los recursos involucrados en su proceso de producción. Así, la ISO/IEC 25012 establece características externas formulando lineamientos para la calidad de los datos almacenados en los sistemas de información (Pinzón y Sanabria, 2013).

La gestión de la calidad es una parte fundamental dentro de cualquier organización que maneja gran variedad de información que depende de los datos con los que se opera. A pesar de ser esto un aspecto sumamente importante para la formulación de información orientada a ayudar en los procesos de toma de decisiones, no suele disponerse de recursos que evalúen la calidad de dichos datos. El modelo expuesto por esta norma, puede entenderse como el grado en que los datos satisfacen los requisitos definidos por la organización a la que pertenece el producto de información y se encuentra compuesto por 15 (quince) características clasificadas en dos grandes categorías. Una de ellas se corresponde con la calidad de datos inherente la cual hace referencia al grado en el que las características de calidad se encuentran intrínsecamente en los datos en sí mismos. Por otro lado, la calidad de datos dependiente del sistema se refiere al grado en el que la calidad es alcanzada y preservada a través de un sistema informático por lo que dependen del dominio tecnológico y se alcanza mediante las capacidades de los componentes de dicho sistema (hardware y software). Finalmente, es posible evidenciar una tercera categoría que contempla ambas características anteriores (Calabrese et al., 2019). Así, y siguiendo a la norma ISO 25012, Calabrese, et al. (2019) agrupan las siguientes características:

Tabla 4.4.: Calidad de los datos. ISO/IEC 25012

a) Calidad de datos inherente.	
Exactitud	Grado en el que los datos representan correctamente el verdadero valor deseado de un concepto o evento en un contexto de uso específico.
Completitud	Grado en el que los datos asociados con una entidad tienen valores para todos los atributos esperados e instancias de entidades relacionadas en un contexto de uso específico.
Consistencia	Grado en el que los datos están libres de contradicción y son coherentes con otros datos en un contexto de uso específico.
Credibilidad	Grado en el que los datos tienen atributos que se consideran ciertos y creíbles en un contexto de uso específico. El concepto de credibilidad incluye al de autenticidad.
Actualidad	Grado en el que los datos tienen la edad correcta en un contexto de uso específico.

Continuación

b) Calidad de datos inherente y dependiente del sistema.	
Accesibilidad	Grado en el que los datos pueden ser accedidos en un contexto específico, particularmente por personas que necesiten tecnologías de apoyo o una configuración especial por algún tipo de discapacidad.
Conformidad	Grado en el que los datos tienen atributos que se adhieren a estándares, convenciones o normativas vigentes y reglas similares referentes a la calidad de datos en un contexto de uso específico.
Confidencialidad	Grado en el que los datos tienen atributos que aseguran que son solo accedidos e interpretados por usuarios autorizados en un contexto de uso específico.
Eficiencia	Grado en el que los datos pueden ser procesados y proporcionados con los niveles de rendimiento esperados mediante el uso de cantidades y tipos adecuados de recursos en un contexto de uso específico.
Precisión	Grado en el que los datos son exactos o proporcionan discernimiento en un contexto de uso específico.
Trazabilidad	Grado en el que los datos proporcionan un camino de acceso auditado a los datos o cualquier otro cambio realizado sobre los datos en un contexto de uso específico.
Comprensibilidad	Grado en el que los datos permiten ser leídos e interpretados por los usuarios y son expresados utilizando lenguajes, símbolos y unidades apropiados en un contexto de uso específico.
c) Calidad de datos dependiente del sistema.	
Disponibilidad	Grado en el que los datos permiten ser obtenidos por usuarios y/o aplicaciones autorizados en un contexto de uso específico.
Portabilidad	Grado en el que los datos permiten ser instalados, reemplazados o eliminados de un sistema a otro, preservando el nivel de calidad en un contexto de uso específico.
Recuperabilidad	Grado en el que los datos permiten mantener y preservar un nivel específico de operaciones y calidad, incluso en caso de fallos, en un contexto de uso específico.

Fuente: elaboración propia en base a Calabrese, et al. (2019)

4.3.3. Determinantes y responsables de la calidad de la información

A rasgos generales puede decirse que la conducción de una organización, así como todos y cada uno de sus propietarios y los distintos actores involucrados en la actividad tienen compromiso con el diseño y el funcionamiento de los sistemas de información. Ese compromiso consiste no solo en participar en ese diseño sino también en asegurar que su funcionamiento sea el adecuado de forma permanente y de garantizar la generación de información suficiente y de calidad necesaria para que cada una de las partes interesadas pueda cumplir con sus roles y responsabilidades (Canetti, 2007).

Siguiendo lo enunciado, puede advertirse que la información y su calidad dependen de tres factores que pueden ser divididos en factores innatos de la entidad, factores discrecionales y

factores ajenos a los anteriores. Los factores innatos son aquellos que se encuentran influenciados por el modelo de negocio, por el entorno en el que opera la organización y por sus características y particularidades propias. Este tipo de factor puede afectar tanto a los usuarios internos como externos y resulta determinante al hablar de sistemas de información dado que, por ejemplo, es de esperar que aquellas organizaciones que poseen sistemas menos sofisticados cuenten con información de menor calidad que aquellas cuyos sistemas presentan mayores niveles de perfeccionamiento. Por otro lado, los factores discrecionales son aquellos que dependen de los incentivos de los directivos de una organización a ofrecer información de calidad. Este tipo de factor es más propenso de afectar a los usuarios externos ya que se encuentra relacionado con los incentivos a la manipulación de la información para reflejar determinados desempeños en beneficio de la dirección. Finalmente, los factores ajenos a las características anteriores son aquellos que tienden a mejorar la parte innata puesto que buscan disminuir la probabilidad de errores en la generación información y registro de las operaciones (errores no intencionales), y la parte discrecional al disminuir la posibilidad de manipulación de la información y de utilización interna o externa por parte de los directivos (errores intencionales). Para este último factor, el control interno constituye un claro ejemplo (Huguet Benavent, 2014).

4.3.3.1. El rol del control interno y de la auditoría

Retomando lo visto en los apartados anteriores, dentro de los conceptos básicos que describen a los sistemas y a sus propiedades, se encuentra el de retroalimentación. Este concepto viene representado por ciertos mecanismos que se encuentran presentes en los propios sistemas y que buscan regular su actividad actuando de manera compensadora cuando necesitan contener o amortiguar desviaciones negativas o bien actuando de manera amplificadora al buscar reforzar determinadas actividades consideradas positivas (Navarro, 2001). Los primeros reciben el nombre de control y no resultan ajenos a los sistemas de información ya que estos también requieren de procesos de supervisión y evaluación encargados de mantener su funcionamiento eficiente teniendo en cuenta sus objetivos.

El sistema de información no solo debe generar información para el exterior sino también para su propia operatoria, de forma que la existencia e interacción de distintos grupos de interés con objetivos disimiles da lugar a advertir que es posible que los intereses de ciertos actores puedan prevalecer sobre los intereses de otros. Los mecanismos de control en el sistema de información tienden, no solo a supervisar las funciones de recolección, almacenamiento, procesamiento y salida de datos sino también a brindar un adecuado balanceo entre estos distintos intereses, con el principal propósito de brindar información objetiva. Sistemas de información carentes de apropiados mecanismos de control

producirán informes faltos de objetividad y confiablidad provocando que el sistema de información que le dio origen pierda por completo la razón de su existencia. De esta forma se hace indispensable reconocer la necesidad de estos mecanismos como un elemento propio de los sistemas de información y como un factor que incide en la confiabilidad y calidad de la información (Canetti, 2007).

El conjunto de mecanismos de control insertos en los procesos y actividades forma parte de lo que se conoce como control interno que, al integrar la totalidad de una organización, se presenta como un concepto indivisible. Autores como Rusenas (2011) reconocen como función y responsabilidad de la dirección la instalación e implementación de este sistema de control interno, de la vigilancia de su correcto y eficiente funcionamiento, de la detección de los desfasajes ocurridos respecto a lo predeterminado y de la adopción de manera oportuna de todas aquellas políticas, normas y procedimientos necesarios para asegurar su correcto desempeño.

El control interno no representa un concepto nuevo ni poco desarrollado, sus orígenes se remontan a épocas de auge industrial donde, como consecuencia del creciente desarrollo, comienzan a separarse las distintas fases empresariales quedando la fase administrativa en un escalón de menor evolución que las fases de producción y comercialización cuyos procesos presentaron avances más acelerados. Con el transcurso del tiempo esta fase administrativa recobra preponderancia y comienza a reconocerse la necesidad de generar e implementar diversos sistemas de control. Debido al crecimiento, los propietarios debieron subdividir y delegar funciones dentro de las organizaciones, así como las respectivas responsabilidades derivadas de las actividades operativas o de gestión. Esta delegación de funciones y responsabilidades necesariamente debió verse acompañada por sistemas o procedimientos tendientes a la protección del patrimonio y a la generación de información coherente y que permitiera una gestión adecuada, correcta y eficiente. Nace así el control interno como una función gerencial de supervisión para asegurar que los planes y las políticas se cumplan tal cual fueron fijados (Rusenas, 2011).

Sin embargo, la visión de control interno tal como la conocemos hoy surge como consecuencia de varios casos de fraude financiero ocurridos en Estados Unidos en los años 80. A raíz de ello, se crea el Committee of Sponsoring Organizations of the Treadway Commission quien se encargó de emitir, en el año 1992, la primera versión del informe “Internal Control - Integrated Framework”, denominado COSO I, con el objetivo de disponer de un marco común que permita a las organizaciones evaluar sus sistemas de control interno.

A raíz de la expansión de este fenómeno, otros países también desarrollaron sus propios marcos conceptuales en lo que a control interno se refiere (informe COCO en Canadá, informe Turnbull en Reino Unido, informe Vienot en Francia, informe King en Sudáfrica, informe Aldama en España, entre otros) pero los posteriores y reconocidos escándalos financieros acaecidos en Estados Unidos, Asia y Europa obligaron a realizar un cambio en el paradigma del control interno, llevando así a la necesidad de establecer normas cada vez más rigurosas. Esto dio lugar, en el año 2002, al dictado de la Ley Sarbanes Oxley que sirvió de marco normativo para imponer sanciones a aquellas entidades públicas que efectuasen manifestaciones positivas sobre la propia estructura de control interno que no reflejen verdaderamente la realidad (Canetti, 2007). Como consecuencia de las nuevas exigencias incorporadas por esta ley, se vio la necesidad de impulsar una revisión a la versión existente del informe COSO surgiendo así la emisión de un nuevo informe. La esencia de este nuevo marco radica en la incorporación del control interno dentro de los procesos de gerenciamiento y de gobierno a fin de que el mismo no sea tratado como un mero ejercicio para el cumplimiento de los requisitos regulatorios, estableciendo así que todos los miembros de una organización poseen compromisos sobre dicho control como parte de su responsabilidad en el logro de los objetivos organizacionales.

Según el objetivo de información del marco enunciado precedentemente, el control interno debe velar por la información generada y acumulada tanto para uso interno como para uso externo por lo que su existencia representa un aspecto importante no solo para garantizar que la misma sea generada acorde a las necesidades y definiciones propias de la organización, sino también para servir de base a aquellas auditorías que buscan dotar de la máxima transparencia posible a la información suministrada a externos (Canetti, 2007).

Gracias a los avances tecnológicos orientados a la información y a las telecomunicaciones, el fenómeno de la sobrecarga informativa ha invadido a las organizaciones provocando que la escasez no se encuentre dirigida a la información sino más bien al tiempo que se requiere para poder procesarla, evaluarla y aplicarla en los distintos ámbitos organizacionales. La planificación de la información busca crear una determinada arquitectura informativa que responda a los objetivos organizacionales a través de un flujo de información basado en las distintas necesidades existentes y que la hagan susceptible a ser utilizada (García, 2006).

Como ha quedo definido, las organizaciones se encuentran sujetas a diversos mecanismos de control que se encuentran abocados a asegurar una correcta gestión y un óptimo uso de sus recursos incluyendo dentro de ellos a los de información. En la medida en que la organización sea más intensiva en el uso de la información, mayor será la importancia de estos recursos, mayor deberá ser el nivel de cultura orientada a la información y

consecuentemente más críticos deberán ser los procesos de auditoría destinados a los mismos. La auditoría orientada a este tipo de recursos no deja de lado la esencia propia de aquellas auditorías que no se encuentran enmarcadas dentro de la órbita financiera y regulada por normativas técnicas. Por el contrario, constituye una auditoría que se encuentra fuertemente vinculada a un activo intangible que presenta grandes dificultades para su valoración, que parte de una idea de diagnóstico, que posee carácter preventivo y corrector, que se aplica sobre procesos sistemáticos y periódicos, que utiliza metodologías no reguladas o estandarizadas sino que más bien se ajustan a las particularidades de cada organización, que debe desarrollarse por profesionales ajenos a las tareas en evaluación y que tiene como propósito la emisión de un conjunto de recomendaciones (Soy i Aumatell, 2003).

Aunque, como se dijo con anterioridad, este tipo de auditorías no obedece a un requerimiento legal o normativo, sino que surge como una práctica que forma parte del control interno, su finalidad se encuentra orientada a construir, mejorar y corregir más que a controlar, velando para que la información que circula por la organización sea la más relevante y apropiada en base a las posibilidades organizacionales. Esto permite evidenciar grandes ventajas que se verán plasmadas en una gestión más racional de los recursos, en la identificación de amenazas de manera inmediata y en una considerable reducción de riesgos, en la accesibilidad y usabilidad de la información por parte de quienes lo requieren debido a su directa orientación al usuario y a la estrategia de la organización, en los cambios culturales para desarrollar estrategias y políticas de información y en la consolidación de esta como un área clave del negocio y no únicamente como una sección de soporte (García, 2006 y Soy i Aumatell, 2003).

Hasta aquí es posible advertir al control interno como una herramienta elemental que ayuda a alcanzar la calidad de la información a niveles internos. Sin embargo, y teniendo en cuenta la existencia de usuarios externos, los organismos reguladores consideran que la calidad de la información puede ser medida en base a si la misma se ajusta o no al espíritu de las normas. Por el contrario, y debido a la numerosa cantidad de fraudes contables que han tenido lugar a lo largo de la historia, es factible considerar que por sí solas estas normas no logran brindar un marco suficientemente abarcativo de calidad y confiabilidad. La existencia de normas contables no asegura per se la emisión de información confiable a los terceros que la utilizan y si bien puede resultar cierto que contribuyen a ese fin, la existencia del sesgo gerencial permite la vulneración de esos objetivos. A raíz de este sesgo y de las asimetrías de la información que pueden tener lugar en estos ámbitos, surge la auditoria externa o contable como medio para brindar confiabilidad a la información orientada al uso externo (Canetti, 2007).

Según lo que establece la Resolución Técnica número 37 (FACPCE, 2013), para que el auditor pueda emitir una opinión sobre los estados contables de un ente o bien abstenerse de emitirla, debe reunir los elementos de juicio válidos y suficientes que respalden su opinión respecto a la información presentada en ellos. Para ello debe obtener un conocimiento apropiado de la estructura del ente, de sus operaciones, de sus sistemas, de su control interno, de las normas legales que le son aplicables y de las condiciones económicas propias y las del ramo de sus actividades. Respecto al control interno del ente, debe evaluarlo siempre que, en relación a su tarea, decida depositar confianza en el mismo. Para ello debe relevar las actividades formales de control interno que son pertinentes a su revisión, comprobar que las actividades formales de control interno se aplican en la práctica y evaluar las actividades reales de control interno comparándolas con las que se consideren razonables en cada circunstancia.

Respecto a la consideración del control interno, la NIA 315 emitida por el International Auditing and Assurance Standards Board (2010) establece que el mismo se diseña, implementa y mantiene con el fin de responder a los riesgos de negocio identificados que amenazan la consecución de cualquiera de los objetivos de la entidad referidos a la fiabilidad de la información financiera, a la eficacia y eficiencia de sus operaciones y al cumplimiento de las disposiciones legales y reglamentarias. A fin de que los auditores puedan considerar el modo en que los distintos aspectos del control interno puedan afectar a la auditoría, el mismo es dividido en cinco grandes componentes a saber:

- El entorno de control.
- El proceso de valoración del riesgo por la entidad.
- El sistema de información, incluidos los procesos de negocio relacionados, relevantes para la información financiera y la comunicación.
- Actividades de control.
- Seguimiento de los controles.

El control interno, por muy eficaz que sea, solo puede proporcionar a la entidad una seguridad razonable del cumplimiento de los objetivos de información. La probabilidad de que estos no se cumplan puede verse afectada por las limitaciones inherentes al control interno que incluyen, tanto los juicios humanos erróneos a la hora de tomar decisiones como el hecho de que el mismo control interno pueda dejar de funcionar debido a los errores humanos. Además, no debe dejarse de lado la posibilidad de que puedan sortearse los controles por colusión entre dos o más personas o por la inadecuada elusión del control interno por parte de la dirección. Adicionalmente, debe tenerse presente que una parte importante de la información utilizada para el seguimiento de los controles puede ser

producida por el mismo sistema de información que está siendo evaluado. Si la dirección asume que los datos utilizados para este seguimiento son exactos sin disponer de una base para dicha hipótesis, los errores que pueden existir en la información podrían llevar a la dirección a conclusiones erróneas derivadas de sus propias actividades de seguimiento. Como consecuencia de ello, resulta necesario tener conocimiento de las fuentes de información relacionadas con esas actividades de seguimiento y la base de la dirección para considerar que esa información es suficientemente fiable para dicha entidad (IASB, 2010).

Tanto los propietarios, como la dirección, los empleados y hasta la propia organización considerada en su conjunto necesitan información relevante para las diversas actividades. Teniendo en cuenta que el sistema del cual proviene esta información puede ser susceptible de captar gran diversidad datos existentes en su ambiente, es imprescindible que dicho sistema sea capaz de brindar toda aquella información que resulte realmente útil y de desechar todo aquello que no presente una importancia relativa. Aunque no resulte una novedad, el principal factor para el éxito de este proceso se corresponde con la dirección y, concretamente, con su compromiso, implicación y liderazgo dado que es a través de ella que podrá desarrollarse una cultura orientada a la información y establecerse metas tendientes a dirigir los esfuerzos necesarios para que esta evolucione hacia una de máxima calidad posible. A nivel interno, es importante comprender que los usuarios toman sus decisiones en base en la información obtenida de los sistemas de información por lo que, si estos consideran que el sistema no es confiable y que sus datos son inexactos, sus dudas se reflejarán en un menor uso del mismo. En contraposición, cuando la satisfacción impacta en un mayor uso, se genera una gran dependencia en el sistema siendo cada vez más necesario encarar actividades que tiendan a protegerlo y mejorar sus niveles de eficiencia y eficacia, generando no solo un caudal de información de calidad que sirva para las distintas actividades internas sino también que posea una alta influencia en la capacidad de la dirección para tomar decisiones adecuadas en cuestiones de dirección y control, así como para preparar informes financieros fiables (González Valiente, 2014)

Establecer que cualquier práctica informativa requiere de garantías de calidad, presupone considerar, además de la responsabilidad de quienes conformen la dirección, la responsabilidad de aquellos profesionales involucrados en el proceso de generación, gestión y control de la información dado que, mediante sus conocimientos y habilidades oportunas, son susceptibles de incidir en la calidad del sistema y de la información generada (González Valiente, 2014). En especial, los controles o auditorias orientadas a la información propiamente dicha, permitirán asegurar que el flujo de información que circule en una organización sea el más relevante y apropiado para ella permitiendo comprender que la

eficiencia y eficacia de un sistema de información se encuentran fuertemente ligadas a las políticas de control interno establecidas (García, 2006).

Adicionalmente, y dada la marcada orientación actual del control interno hacia la administración de los riesgos de negocio, este se vuelve indispensable para identificar aquellos hechos potenciales que pueden afectar a la totalidad de la entidad. La evaluación de los riesgos consiste en la identificación y análisis de los riesgos relevantes a la ejecución de los objetivos y se considera que, en la dinámica actual de los negocios una de las principales cuestiones que requiere especial atención se encuentra relacionada con los avances tecnológicos (Estupiñan Gaitán, 2015).

Las tecnologías de la información y telecomunicaciones presentan constantes avances que se encuentran estrechamente vinculados a los sistemas de información. El procesamiento electrónico de datos como parte y eje fundamental de estos avances, si bien influye en la disminución de algunos riesgos asociados al manejo manual de datos y de información, también inserta una nueva categoría de riesgos que no puede ser ignorada y que debe ser necesariamente alineada a los riesgos de negocio y ser tenida en cuenta por los profesionales al planificar sus respectivas labores de auditoría (Canetti, 2007).

5. Capítulo III: Pautas propuestas para una auditoria de sistemas de información mediados por tecnología

Al estar la tecnología tan presente en todas y cada una de las áreas de una organización, es un requisito fundamental para quien realizará evaluaciones de un sistema de información, estar actualizado en esta temática y conocer los riesgos que todo proceso tecnológico trae al proceso de información. Frente a ello, y a fin de abarcar la problemática de manera oportuna, el trabajo del auditor debe encaminase hacia la evaluación de aquellos controles que una organización posee frente a su propia estructura tecnológica y trabajar a partir de sus políticas de seguridad, de la organización de sus sistemas, del almacenamiento de la información y de las medidas de respuesta frente a los diversos incidentes que pueden presentarse en dicho contexto. El auditor debe asegurarse que sus revisiones abarquen las diversas herramientas tecnológicas existentes en la organización a fin de garantizar su uso, administración y funcionamiento adecuados (Klus, 2018).

Según lo establecido por MCCafferty (2017) y a pesar del devenir tecnológico, la auditoría centrada en las tecnologías de la información continúa siendo un ejercicio que se encuentra opacado y muchas veces subestimado, prevaleciendo en mayor medida las propuestas e implementaciones que surgen como consecuencia de la auditoría externa, que aquellas medidas que puede ofrecer la propia auditoría interna.

Si bien es notoria, según lo observado a raíz de las entrevistas, la inclinación por parte de los auditores en considerar como aspectos claves actividades tendientes al conocimiento de la estructura del sistema que da soporte a la actividad o proceso a ser evaluado, al análisis de la segregación de funciones así como de los perfiles, accesos, políticas de usuario y contraseñas, al análisis de registro de actividad de los usuarios, a la prueba de algunos controles implementados en los sistemas y considerar presenciar los procesos a ser evaluados, existen otros aspectos poco reconocidos como claves o dotados de la importancia que merecen frente al contexto considerado. Ejemplo de ello son aquellas actividades tendientes a la verificación de la existencia de narrativa de controles tanto automáticos como manuales y flujogramas de los mismos, la comprobación del correcto establecimiento de parámetros dentro de los sistemas y cómo estos son respetados por los usuarios, el análisis del conocimiento que el usuario posee sobre el sistema que opera así como su capacidad para operar con el mismo, la existencia de políticas de continuidad de servicio, el grado de dependencia a los sistemas mediados por tecnología, entre otros.

La actuación de los profesionales en Ciencias Económicas ha sido objeto de numerosas y detalladas regulaciones encontrándose sujeta a diversos estándares de cumplimiento tales

como resoluciones emitidas por la FACPCE y los Consejos Profesionales, normas internacionales de contabilidad y auditoría, circulares, entre otros. Sin embargo, existen áreas donde aún no se poseen definiciones ni regulaciones contundentes y donde la definición del alcance de la revisión de auditoría se encuentra difuminada y muchas veces es objeto de confusión y desconocimiento. La auditoría interna representa una rama interdisciplinaria y aunque los temas que abordan los aspectos tecnológicos y a la preservación de información suelen ser gestionados por especialistas en dichas disciplinas, generalmente se realizan bajo la supervisión y liderazgo de profesionales en Ciencias Económicas. Es por ello que la propuesta desarrollada en el presente capítulo busca establecer los lineamientos necesarios para realizar una auditoría de sistemas de información mediados por tecnología buscando influir de manera positiva en la calidad de la información generada por una organización, tanto en la utilizada a nivel interno como aquella que es expuesta a terceros a través de los estados contables o financieros.

5.1. Esquema de la propuesta

La propuesta desarrollada tiene como marco principal la metodología establecida por el informe COSO donde se establece que los objetivos del control interno se encuentran relacionados con las operaciones, la información y el cumplimiento de leyes y reglamentaciones. Siguiendo los objetivos de información, y teniendo como pilares a los cinco componentes interrelacionados del control interno, se desplegará una serie de sugerencias que, partiendo del conocimiento de la organización, permitirán comprender y evaluar las distintas funciones de su sistema de información así como garantizar, a niveles mínimos, la calidad del flujo de información que corre a través de ella considerándola, no solo una herramienta esencial para la toma de decisiones sino también, un elemento de entrada para otros procesos o actividades internas. Estos cinco componentes pueden resumir en:

- Ambiente de control.
- Evaluación de riesgos.
- Actividades de control.
- Información y comunicación.
- Supervisión, seguimiento o monitoreo.

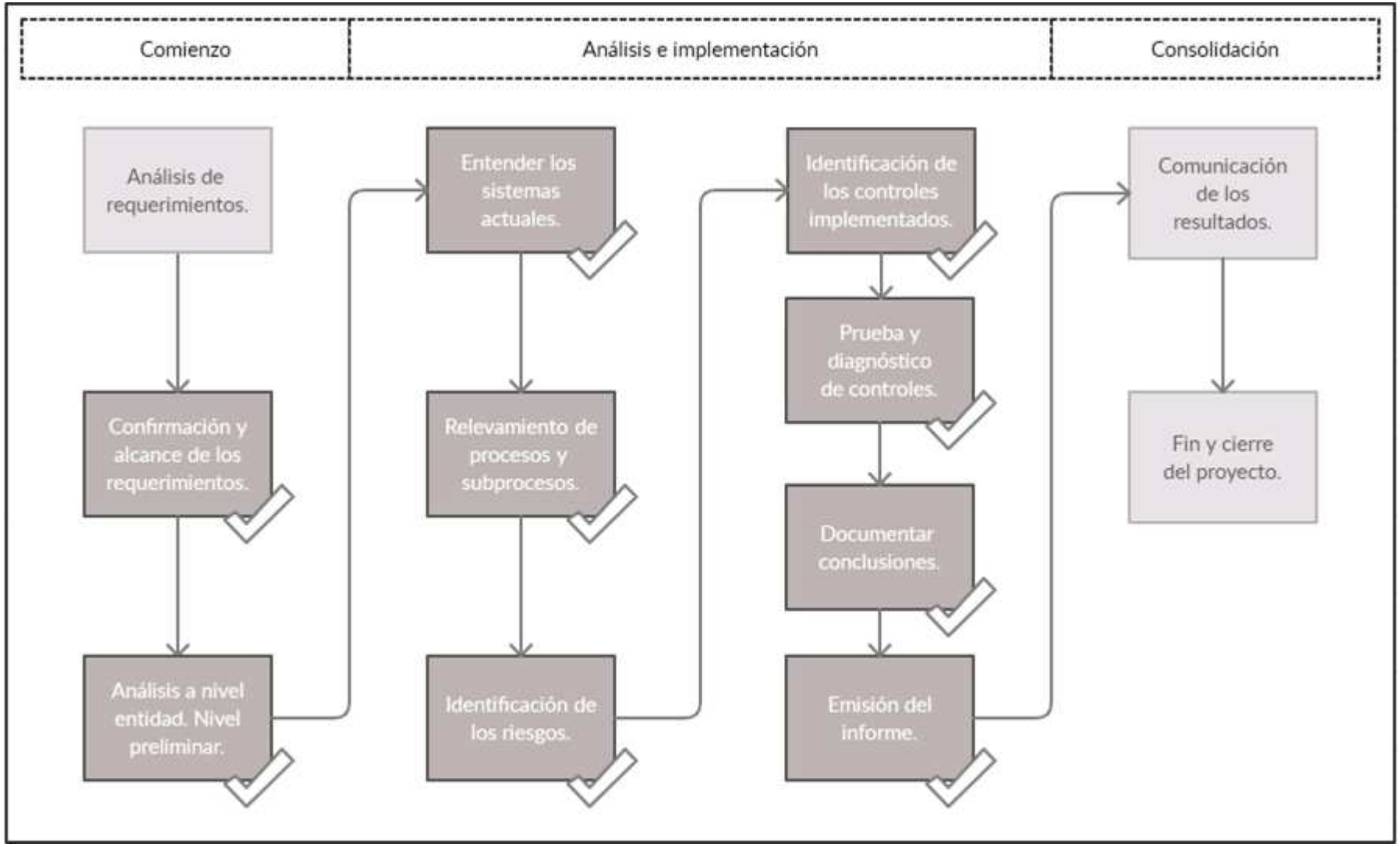
Adicionalmente y como complemento, se toma como referencia a los marcos de negocio para el gobierno y la gestión de las tecnologías de información, COBIT 4.1 y COBIT 5 (IT Governance Institute, 2007 y IT Governance Institute 2012), a fin de enfocarnos en la gestión de la estructura tecnológica que las organizaciones utilizan para el desarrollo de

todos sus procesos generadores de información. La utilización de estos marcos particulares para el desarrollo de este trabajo encuentra su justificación en que los mismos son mundialmente considerados como una sólida herramienta para aquellas organizaciones que buscan crear valor mediante el uso de las TI y a su vez optimizar los niveles de riesgo, impulsando a que las tecnologías de la información se administren de manera holística en todos sus niveles y abarcando los distintos procesos de negocio de principio a fin.

Tomando como cimientos los principales problemas identificados como consecuencia de la revisión documental, las entrevistas realizadas a los diversos profesionales referentes en la temática tratada y las recomendaciones efectuadas por entidades como el CPCECABA (2013) y por The Institute of Internal Auditors (2007), se ha elaborado una propuesta de lineamientos para una auditoría de sistemas de información mediados por tecnología. Estos lineamientos se encuentran plasmados en un diagrama de flujo que resume el proceso propuesto y del cual surgen las distintas actividades a ser abordadas por el auditor. Adicionalmente, y como consecuencia de la necesidad de una clara definición de las tareas de revisión en el contexto mencionado, se describirá el alcance de las principales fases de la propuesta.

El proceso se encuentra dividido en tres etapas iniciando por la etapa de comienzo donde se analizará el alcance de la tarea a realizar, los tiempos requeridos y la posibilidad de su cumplimento, siguiendo por una primera obtención de información general de la organización. Esta etapa se encuentra conformada por las fases de: 1) confirmación y alcance de los requerimientos y 2) análisis a nivel entidad, nivel preliminar. La siguiente etapa, análisis e implementación, se encuentra abocada al conocimiento de la estructura, utilización e importancia de los sistemas dentro de la organización, así como la evaluación de los controles involucrados en las actividades de generación de información, tomando como base los procesos a ser evaluados e incluidos dentro del alcance. Así, la etapa de análisis e implementación abarca las siguientes fases: 3) entender los sistemas actuales, 4) relevamiento de procesos y subprocesos a evaluar, 5) identificación de los riesgos en base a los procesos relevados y a las etapas, 6) identificación de controles implementados en base a los riesgos, 7) prueba y diagnóstico de controles, 8) documentar conclusiones y emisión del informe final. Finalmente, la etapa de consolidación representa el cierre del proceso donde el auditor puede comunicar las conclusiones obtenidas y plasmadas en su informe, así como las oportunidades de mejora detectadas como consecuencia de la tarea realizada. A continuación, se presenta el diagrama de flujo del esquema propuesto, dividido en función de las etapas mencionadas y de las fases que las conforman.

Figura 5.1. Diagrama de flujo del esquema propuesto



Fuente: elaboración propia.

5.2. Etapa de comienzo

El trabajo de auditoría iniciará con la etapa de comienzo, donde, luego del análisis de los requerimientos o especificaciones técnicas realizados por la organización a ser auditada, deberán analizarse aspectos como el alcance mínimo de la tarea a realizar, los tiempos requeridos de trabajo y entrega de informes, su posibilidad de cumplimiento en función del equipo de trabajo del auditor, las condiciones específicas requeridas, entre otros. A su vez, y a los fines de sentar las bases para la planificación de la tarea y cronograma de auditoría, deberá realizarse una primera obtención y relevamiento de información general de la organización.

5.2.1. Confirmación y alcance de los requerimientos

Los sistemas de información abarcan la totalidad de una organización por lo que su estructura puede ser tan amplia como diversa a lo largo de la misma entidad. Es por ello que el primer lineamiento se relaciona con el entendimiento de los límites establecidos por el alcance del trabajo a realizar. Suponer que en un mismo trabajo de auditoría será posible evaluar todo el sistema de información, implicaría estudiar a la organización en su totalidad, situación que puede verse limitada por los propios recursos del auditor y por el tiempo estipulado en los requerimientos (Juergens, 2006).

En una primera instancia resulta vital entender que el alcance de la auditoria puede estar orientado a un área o sector determinado incluyendo determinados procesos y subprocesos, así como las diversas influencias que estos pueden poseer en otras áreas, sectores, procesos o actividades. En este sentido, un alcance más amplio podría requerir sucesivos trabajos de menor alcance en vez de encontrarse abarcado en solo uno, siendo lo más adecuado acotar el perímetro a auditar dado que, realizar diferentes y continuados trabajos de auditoria podría ser más efectivo que intentar abarcar varios procesos y sus aplicaciones en una sola totalidad (Instituto de Auditores Internos de España, 2020).

Por otro lado, es necesario resaltar que en algunas situaciones la demarcación de los límites quedará en manos de mismo auditor siendo su propia perspectiva la que fijará la extensión de dicho alcance, acotando o ampliando los elementos y relaciones a ser analizados (Volpentesta, 2004). Siguiendo lo expuesto, es importante destacar que, si bien una auditoría de este tipo puede tener una perspectiva parcial al estar focalizada en una determinada unidad de información, función o proceso particular, dado su alcance integral, busca realizar un diagnóstico e incidir en un aspecto crítico al afectar al proceso de generación de información y su comunicación (Soy i Aumatell, 2003). En base a esto, en

esta etapa se propone realizar una identificación preliminar de los procesos y subprocesos incluidos en los requerimientos, con el objetivo de identificar la dependencia y relaciones con otras áreas, procesos, subprocesos o actividades, el orden que las unifica y cualquier otro aspecto que resulte importante y que pueda influir en la fijación de los límites por parte del auditor. A tal fin, y siguiendo a García (2006) y Soy i Aumatell (2003), en esta etapa se propone:

1) Examinar todas las funciones organizacionales que se encuentran relacionadas con la información del área, proceso o subproceso a ser auditado y determinar cómo estas la utilizan. Esta actividad puede realizarse en base a distintos procedimientos tendientes a analizar la ruta de la información arriba-abajo partiendo de niveles superiores hasta llegar a los inferiores, la ruta abajo-arriba cuando se comienza con los niveles inferiores hasta llegar a los superiores y la ruta dentro-fuera en donde se puedan identificar oportunidades y riesgos.
2) Identificar quienes son los usuarios internos de la información generada por el área, proceso o subproceso a evaluar, ver cómo la utilizan y para qué y conocer sus distintos requerimientos, así como sus prácticas y comportamientos respecto a ella.
3) Analizar las necesidades actuales y el uso de la información relacionadas con el área, proceso o subproceso a evaluar buscando determinar los flujos de información dentro de la organización y las interrelaciones, es decir, quién proporciona información a quién y cómo esta es obtenida por las personas para desarrollar sus tareas, identificar qué información necesitan y producen los distintos procesos o subprocesos involucrados con el objeto de auditoría, en qué medida la necesitan y para qué, ver de dónde procede dicha información, identificar quién la crea, a quién pertenece, quién se ocupa de su calidad y si es o no fácil de obtener y utilizar. Esta actividad tiene como objetivo identificar aquellas salidas de un proceso o subproceso que pueden resultar entradas de un proceso o subproceso posterior.

Estas actividades buscarán enmarcar la actividad del auditor, ayudarlo a delimitar el alcance de su tarea y conocer las relaciones y conexiones que las distintas actividades poseen sobre y como consecuencia de la unidad a ser auditada. De esta manera, dentro de esta etapa comienza el desarrollo del programa de trabajo que se inicia con un primer entendimiento de las actividades o procesos que deberán auditarse, así como la determinación del momento en que serán auditados, del tiempo estimado requerido según el alcance planeado y según la naturaleza y extensión del trabajo realizado por otros auditores o en otras auditorías, en caso de existir. Adicionalmente, el profesional debe tener presente que el programa deberá permitir la suficiente flexibilidad para cubrir demandas imprevistas y que surjan como consecuencia de situaciones no contempladas previamente (Echenique García, 2001).

5.2.2. Análisis a nivel entidad. Nivel preliminar

El análisis o revisión preliminar constituye un requisito mínimo de trabajo que sirve de base para la planificación de cualquier auditoría y tiene como propósito el conocimiento de la organización buscando identificar sus objetivos, estrategias, modelo de negocio y todos aquellos procedimientos y métodos establecidos para poder alcanzarlos. Esto permitirá al auditor identificar aspectos críticos de la organización como los bienes y/o servicios que provee, sus bases de mercado, su cadena de suministro, sus procesos de producción, entre otras características propias. Con dicho análisis, el auditor podrá hacerse de un panorama preliminar que le ayude a identificar la información necesaria para el cumplimiento de las actividades organizacionales, los flujos necesarios de información a lo largo de su estructura, los riesgos de negocio, a comprender cómo la tecnología sirve de soporte al modelo de negocio desarrollado y cómo la organización busca mitigar sus riesgos (Rehage, Hunt y Nikitin, 2008).

Frente a este panorama, el auditor debe considerar, además de la evaluación del entorno operativo, la evaluación del ambiente o entorno de control entendiendo que todas las actividades de control aplicadas por la entidad deben encontrarse sobre las personas, en cualquier parte de los sistemas, sobre los procesos, funciones o actividades y no representar una entidad separada de dichos elementos. El objetivo de conocer el ambiente de control consiste en determinar la existencia de un ambiente de control positivo y no basado puramente en la confianza dado que este marca las pautas de comportamiento de la organización, proporcionando disciplina y estructura e influenciando de manera directa en el nivel de concientización del personal respecto a los procesos y mecanismos de control. En este sentido, el auditor debe tener presente que todo el personal es responsable por las tareas de control destinadas a identificar aquellas circunstancias que dificultan o retrasan las actividades que se encuentran bajo su órbita (Estupiñan Gaitán, 2015).

De esta forma, y entendiendo que la complejidad del entorno de control tendrá efecto directo en el perfil de riesgo general del ente, el profesional deberá evaluar aquellos mecanismos que hacen a dicho ambiente (Rehage et al., 2008). Siguiendo a Estupiñan Gaitán (2015), Rusenas (2011) y a Cansler (2003) se propone la siguiente guía para el análisis y evaluación del ambiente de control.

Tabla 5.1.: Guía para una primera evaluación del ambiente de control

Nro	Actividad	Comentarios
1	Indagar sobre la existencia e implementación de códigos de conducta, códigos de ética, reglamentos del personal u otras políticas orientadas a prácticas de negocio aceptables, a conflictos de interés y a estándares esperados de comportamiento ético y moral. Indagar sobre la correcta comunicación de estas políticas a fin de observar si la organización se encuentra orientada a prácticas altamente influenciadas por el plano ético.	
2	Indagar sobre la existencia de manuales de procedimiento escritos o, en su defecto, descripciones informales de trabajo que detallen cada actividad en particular y que contengan una descripción de cómo debe ser desarrollada desde el inicio hasta su final, de forma que permitan conocer la lógica de las tareas, evitar posibles inconsistencias o dudas en la operatividad y reducir la probabilidad de decisiones incorrectas o de mala calidad. Revisar si se encuentran acompañados de cursogramas, diagramas de flujo, formularios intervinientes e instrucciones.	
3	Consultar sobre el establecimiento formal de los objetivos alcanzables de desempeño, así como la existencia y comunicación de sanciones frente a fraude o incumplimiento de los procedimientos considerados aceptables para las tareas a ser desarrolladas.	
4	Indagar sobre la existencia de análisis formales y adecuados respecto a las habilidades y conocimientos necesarios para desempeñar adecuadamente las tareas encomendadas.	
5	Indagar sobre la existencia de un área específica de control o auditoria interna independiente de la administración y la frecuencia y oportunidad de sus reuniones, así como el asentamiento formal de las mismas a través de actas donde consten las decisiones o medidas a ser implementadas, entre otras.	
6	Consultar sobre la suficiencia y oportunidad mediante la cual el área de auditoría proporciona información para el monitoreo de los objetivos y estrategias organizacionales, así como la suficiencia y oportunidad mediante la cual esta área recibe información sensible, investigaciones y actos impropios.	
7	Consultar sobre la definición y asignación de las responsabilidades claves de los administradores y de los conocimientos y experiencias en relación a dichas responsabilidades. Indagar respecto a la delegación de autoridad para cumplir con las metas y objetivos incluyendo responsabilidad por los sistemas de información.	
8	Indagar sobre la existencia de estándares y procedimientos relacionados con el control, incluyendo descripciones de las actividades de control a ser desarrolladas por parte del personal.	
9	Indagar sobre el número apropiado de empleados para las diversas actividades, particularmente con respecto al procesamiento de datos, a los niveles de habilidades requeridos relativos al tamaño de la entidad y a la naturaleza y complejidad de las actividades y sistemas (análisis de la carga operativa).	

Fuente: elaboración propia.

5.3. Etapa de análisis e implementación

Esta etapa se encuentra abocada al entendimiento del proceso de generación de información debiendo analizarse y evaluarse su ciclo y todo el contexto donde el mismo es desarrollado. Esta etapa inicia con un primer entendimiento de los sistemas y del instrumental tecnológico que da soporte a las diversas actividades y procesos a ser auditados, sus riesgos y la evaluación de sus diversos mecanismos de control.

5.3.1. Entender los sistemas actuales

La estructura, utilización e importancia de los sistemas por parte de las organizaciones es casi tan diverso como la cantidad de organizaciones existentes. Así, es posible evidenciar organizaciones donde los sistemas son vistos como un mero instrumento destinado a la emisión de documentos como facturas, recibos y reportes requeridos legalmente mientras que otras, además, utilizan dichos sistemas como fuente indispensable para la obtención de información estratégica y valiosa. En este último caso, los sistemas pueden representar un verdadero desafío para el auditor dado el cúmulo de información generada en base a los datos maestros, a las diversas clases de documentos, al tipo de transacciones, entre otros (CPCECABA, 2013).

Por otro lado, los avances tecnológicos han generado la posibilidad de captar, procesar y exponer mayor cantidad de información a menor costo y en menor tiempo. Estos cambios no son ajenos al diseño y funcionamiento de los sistemas de información en general ni a la actividad contable en particular, de forma que estas tecnologías han generado cambios no solo en los medios de registro sino también en los diversos mecanismos de control (Canetti, 2007). Frente a estas situaciones planteadas, el auditor debe comprender el avance tecnológico involucrado en los sistemas de información del ente a través del entendimiento de su universo tecnológico o TI, así como la importancia que dichos sistemas poseen para las áreas, sectores o procesos objeto de auditoría.

5.3.1.1. Entender el universo TI

Cada ambiente TI representa un ambiente único que trae aparejado un determinado conjunto de riesgos. La diversidad en los ambientes tecnológicos hace difícil, sino imposible, el armado de un plan genérico y universal orientado a las tecnologías de la información de forma que, para ser efectivo, el auditor debe crear un plan de auditoria específicamente basado en las necesidades y características propias de cada ambiente particular. Para ello resulta necesario para el auditor obtener una adecuada comprensión de los sistemas, aplicaciones y estructura TI (bases de datos, sistemas operativos, redes, ambiente físico, entre otros) que dan soporte a las áreas o sectores a ser auditados buscando entender qué tan dependiente de las tecnologías de información es organización al momento de procesar las transacciones bajo análisis (Juergens, 2006 y Rehage et al., 2008).

Siguiendo las recomendaciones de CPCECABA (2013) y Rehage et al. (2008), en esta etapa, el auditor debe considerar:

- El grado de centralización de los sistemas y recursos TI. Esto afecta en la funcionalidad de la estructura TI dado que, por ejemplo, en las organizaciones más grandes, complejas y descentralizadas, mayor descentralización se encontrará en las operaciones TI y mayor podría ser la cantidad de aplicaciones desarrolladas a medida y utilizadas por la organización. Mientras que, en aquellas organizaciones más pequeñas, simples y centralizadas, mayor será la centralización de las operaciones TI y el auditor podría encontrarse con sistemas enlatados o estandarizados.
- La estructura tecnológica utilizada, el uso de tecnologías emergentes y el nivel de conocimientos técnicos específicos requeridos al personal TI (en caso de existir).
- El nivel de desarrollo y mantenimiento interno de las aplicaciones a ser utilizadas o su nivel de tercerización, así como el grado de complejidad de las mismas.
- Servidores que contienen las aplicaciones críticas de la organización, la forma de acceder a ellos y quienes pueden hacerlo, así como el sistema operativo de los mismos y su estado de actualización.
- Mapa de red que posea una identificación sobre los puntos de acceso lógico, de los dispositivos de conectividad y seguridad implementados, así como cualquier otra información al respecto y la forma en que los usuarios se conectan a la red y a las aplicaciones tanto de manera local como remota.
- Información sobre las aplicaciones relevantes para las tareas a ser analizadas, funcionalidad, complejidad y el modo en que capturan y registran todos los eventos correspondientes.
- Grado de estabilidad y seguridad de las aplicaciones en función de su naturaleza (leguaje de programación, desarrollo propio o software comercial, disponibilidad de código fuente, personal de sistemas con acceso lógico y habilidades para efectuar modificaciones, documentación de modificaciones, período de tiempo transcurrido desde la última modificación, entre otros) y grado en que los datos son integrados o compartidos entre aplicaciones a nivel general.

A medida que las organizaciones evidencian mayor dependencia en la disponibilidad e integridad de las tecnologías de información para llevar acabo sus operaciones y para cumplir con sus objetivos, mayor será la importancia que los riesgos TI tendrán en el perfil de riesgo general de la organización (Rehage et al., 2008). Como consecuencia de ello, y una vez comprendido el universo TI, es importante que el auditor analice y revise cómo la entidad administra el riesgo tecnológico que deriva de su propia estructura tecnológica. A tal fin, se propone el siguiente *checklist* para la revisión de dicha administración cuyo contenido se encuentra basado en manuales de buenas prácticas establecidos por la Red Global de Conocimientos en Auditoría y Control Interno, Estupiñan Gaitán (2015) y Rusenas (2011).

Las preguntas enunciadas a continuación no pretenden cubrir la totalidad de las situaciones que pueden presentarse, por lo que pueden eliminarse o adicionarse las que se consideren necesarias en función del objetivo de la evaluación y de las características propias de la entidad.

Tabla 5.2.: *Checklist* para la identificación del marco de control interno

Nro	Pregunta	Sí	No	N/A	Comentarios
1	¿Dispone la organización de un área, departamento o funcionario de alto nivel encargado de la estructura informática?				
2	¿Se revisan de manera periódica las funciones y responsabilidades definidas para el personal informático? ¿Con qué frecuencia?				
3	¿Posee la organización un detalle de aquella información cuya pérdida pueda tener un gran impacto en su operatividad? ¿Cuál es dicha información?				
4	¿Los documentos de la organización se encuentran clasificados de acuerdo a su criticidad? ¿Se encuentran debidamente protegidos?				
5	¿Existe algún responsable de administrar el riesgo relacionado con la tecnología? ¿Quién es dicho responsable?				
6	¿Se han desarrollado actividades tendientes a identificar riesgos relacionados con la tecnología, así como a identificar las acciones para su mitigación?				
7	¿Se han identificado cuáles de esos riesgos son de mayor impacto y probabilidad, así como sus costos? ¿Cuáles son dichos riesgos?				
8	¿Se posee conocimiento sobre las amenazas a los datos e información de la organización? ¿Cuáles son dichas amenazadas?				
9	¿Cuenta la organización con un programa de seguridad frente a amenazas internas y externas?				
10	¿Existe algún responsable frente a la presencia de una amenaza interna o externa que pueda derivar en la pérdida de información? ¿Quién es dicho responsable?				
11	¿Se evalúan de manera periódica los controles implementados frente a los riesgos relacionados con la tecnología?				
12	¿La organización ha implementado mecanismos que mitiguen específicamente los ataques cibernéticos?				
13	¿Se analizan los riesgos y el impacto en la actividad frente a cambios en la estructura tecnológica?				
14	¿Los objetivos estratégicos TI se encuentran alineados con los objetivos estratégicos de negocio?				

Continuación

Nro	Pregunta	Sí	No	N/A	Comentarios
15	¿Posee la organización procesos relacionados con riesgos derivados de la tecnología? ¿Cuáles son dichos procesos? ¿Se encuentran gestionados de principio a fin?				
16	¿La organización cuenta con políticas para gestionar el riesgo relacionado con la tecnología? ¿Se encuentran dichas políticas vigentes?				
17	¿La organización cumple con las condiciones técnicas necesarias que posibiliten el acceso a seguros contra ciberriesgos?				
18	¿La organización cuenta dentro de su presupuesto con recursos para invertir en la seguridad de los datos?				
19	¿La cultura de la organización promueve considerar la gestión de los riesgos relacionados con la tecnología en el personal?				
20	¿El personal desarrolla programas de capacitación en la gestión de riesgos incluyendo riesgos tecnológicos o digitales?				
21	¿Se incluye a la seguridad física dentro de la gestión de riesgos?				
22	¿Los riesgos son revisados y analizados conjuntamente con los usuarios de los sistemas o aplicaciones?				
23	¿Se poseen políticas de continuidad de negocio frente a la caída de los servicios de los diversos sistemas o aplicaciones? ¿Se encuentran esas políticas vigentes? ¿Las mismas han sido comunicadas a la totalidad del personal?				
24	¿Se han realizado simulaciones de incidentes con el objetivo de evaluar los planes de respuesta y de recuperación?				
25	¿Se ha contratado con anterioridad a terceros para evaluar la efectividad de los controles establecidos frente al riesgo relacionado con la tecnología?				
26	¿Se realizan análisis periódicos de vulnerabilidad del hardware y especialmente de servidores?				
27	¿Se da cumplimiento a la legislación vigente que regula la seguridad en la información y la protección de datos?				

Fuente: elaboración propia.

Los riesgos relacionados con la tecnología se encuentran representados por la posibilidad de que ocurra un evento asociado con el contexto tecnológico de la organización (uso, propiedad, operación, participación, influencia y adopción de TI) y que afecte adversamente el logro de los objetivos. Aunque no existe una clasificación genérica sobre este tipo de

riesgos dada su amplitud, el mismo se encuentra anclado a las características propias de las organizaciones, al tipo de tecnología que utiliza y a los procesos a los que esta se encuentra relacionada. La incorporación de tecnología de la información en las organizaciones no encuentra punto de retorno por lo que, la decisión de incorporarla en los procesos de negocio para obtener mejores resultados trae consigo la necesidad de administrar los riesgos que de ella pueden derivar (Fuenzalida Contreras y Ambrosio Pradel, 2011).

Visto de este modo, el auditor debe tener presente que el riesgo tecnológico no puede ser entendido como un riesgo independiente del modelo de negocio, encontrándose condicionado tanto por los factores técnicos como por factores humanos. Según lo establecido por el Instituto de Auditores Internos de España (2014), los factores técnicos derivan del progreso asociado a la demanda de soluciones complejas en mercados cada vez más competitivos y que, de no ser afrontados de manera adecuada, pueden tener un impacto negativo en la organización. Por otro lado, las organizaciones se encuentran compuestas por personas con motivaciones y capacidades heterogéneas provocando muchas veces que el mayor riesgo derive del propio usuario ya sea como consecuencia las actividades malentendidas o de los errores involuntarios.

5.3.1.2. Entender el uso del sistema de información incluyendo el contable

Como se dijo con anterioridad, el auditor debe incluir dentro de su alcance las diversas influencias (o alguna de ellas) que los procesos auditados poseen en otras áreas, sectores, procesos o actividades. Un ejemplo de ello lo representan aquellas estimaciones que se basan en TI y que sirven para determinar la antigüedad de cuentas por cobrar, de inventarios de lento movimiento, depreciaciones, antigüedad de empleados para determinar sus beneficios laborales, flujos futuros, proyecciones, entre otras y que serán posteriormente utilizados para ciertos registros contables (Holguín Maillard, 2014).

De esta forma para entender cómo es utilizado el sistema de información, y teniendo como marco las áreas o sectores auditar y las aplicaciones que estas utilizan, podría ser necesario incluir un análisis del sistema contable ya que mucha de la información generada en estas áreas o sectores puede tener influencia directa en la información destinada a terceros. Con dicho objetivo y tomando como referencia lo establecido por CPCECABA (2013), se propone el siguiente *checklist* para comprender la influencia sobre el sistema de información contable.

Tabla 5.3.: *Checklist* para comprender la influencia sobre el sistema contable

Nro	Pregunta	Sí	No	N/A	Comentarios
1	¿Se posee un detalle de todas las transacciones que sean importantes para los sectores o áreas a auditar y que se encuentren relacionadas con las aplicaciones a ser evaluadas?¿Cuáles son dichas transacciones? Indagar sobre las mismas.				
2	¿Se encuentran procedimientados todas las actividades o procesos tanto manuales como automatizados por medio de los cuales estas transacciones se inician, se registra, se procesan, se corrigen en caso de ser necesario y se transfieren al sistema contable?¿Cuáles son esas actividades o procesos? Indagar sobre los mismos.				
3	¿Se poseen descripciones e indicaciones sobre los registros contables relacionados, la información respaldatoria y las cuentas específicas que se emplean para iniciar, registrar, procesar e informar transacciones? Indagar sobre los mismos.				
4	¿Se poseen descripciones e indicaciones para la corrección de información errónea y el modo en que la misma se transfiere a los libros mayores? Indagar sobre los procedimientos.				
5	Los registros que se realizan en los libros diarios y mayores, ¿se encuentran totalmente automatizados y estandarizados o algunos se realizan de manera manual?¿Cuáles son dichos registros manuales y por qué motivo se realizan de ese modo?				
6	¿Se poseen descripciones o indicaciones sobre la forma en que el sistema de información capta los hechos no transaccionales que son importantes para los estados contables, para otros informes para la toma de decisiones o reportes para los organismos de contralor? Indagar sobre el procedimiento.				
7	¿Se poseen descripciones e indicaciones para la confección de los estados contables, incluyendo las estimaciones contables significativas, los criterios de valuación, los hechos posteriores al cierre? Indagar sobre el procedimiento.				
8	¿Se realizan controles sobre las registraciones y los asientos no estandarizados utilizados para registrar operaciones o ajustes inusuales que tengan como origen reportes emitidos por las aplicaciones específicas? Indagar sobre los distintos procedimientos.				

Fuente: elaboración propia.

5.3.2. Relevamiento de procesos y subprocesos a evaluar

Entendido el contexto tecnológico imperante en los sistemas de la organización y cómo estos son utilizados, el auditor debe centrarse en el o los procesos y subprocesos a evaluar y que forman parte de la delimitación realizada al inicio de su trabajo. Es importante contar con la mayor cantidad de información posible de estos procesos y subprocesos como ser descripciones de los mismos, cursogramas, procedimientos y actividades que los

componen, instructivos existentes, documentación respaldatoria y cualquier otra información que ayude a entender su trascendencia y características. Para ello deberán utilizarse técnicas que permitan entender la secuencia y el camino a seguir para llevarlos a cabo. Dichas técnicas, según Cansler (2003) pueden consistir en:

- Entrevistas a los empleados que tengan a su cargo la realización de las distintas actividades y tareas de los procesos y/o subprocesos para entender la operatividad.
- Inspección de documentos que respalden las actividades y los registros.
- Pruebas de recorrido o *walkthrough* que consisten en seguir una o más transacciones desde el inicio hasta llegar al final a través de un informe o reporte (ya sea estados contables, financieros o informes internos).
- Indagaciones sobre el sistema informático utilizado para la gestión de la información bajo análisis a nivel transaccional.

Para lograr este objetivo, el auditor necesita dividir los procesos en una serie de tramos, identificando los componentes que realizan las actividades básicas de cada uno, evaluar la confianza de cada componente y en forma agregada, evaluar la confianza total del sistema que soporta a dicho proceso (Echenique García, 2001). Siguiendo las funciones de los sistemas de información que fueron desarrolladas en el capítulo anterior, para cada proceso o subproceso objeto de auditoría, se propone el análisis en función de los siguientes tramos:

- Recolección de elementos de entrada: captación y registro de datos.
- Almacenamiento de datos: archivo, clasificación y recuperación de datos.
- Procesamiento de datos en información: análisis, cálculos, organización de datos, entre otros.
- Salida de productos de información: comprensión, transmisión y exposición de datos.

El objetivo consiste en poder dividir los procesos o subprocesos en cuatro niveles a fin de estructurar el análisis de auditoría de forma que el mismo permita un enfoque específico. Esto permitirá además, analizar si los contenidos son adecuados en base a las necesidades de los procesos y subprocesos, facilitará la posibilidad de evaluar la información teniendo en cuenta el grado de eficiencia y eficacia en función de su utilización y su distribución, establecer una arquitectura de los contenidos y la forma más adecuada para gestionarla (pautas para la creación de la información, selección, clasificación, distribución, entre otros), determinar qué información es relevante, esencial o imprescindible, por qué y para quién, cuál es susceptible de ser protegida y cuál difundida, así como identificar la información crítica, cómo se la utiliza y comparte y evaluar los procedimientos que se realizan para resguardar su confidencialidad (García, 2006 y Soy i Aumatell, 2003).

5.3.3. Identificación de los riesgos en base a los procesos relevados y etapas

Como se expresó en apartados anteriores, la extensión y naturaleza de los riesgos varían en función del sistema de información de la entidad y del instrumental tecnológico que lo sustenta. A partir de la comprensión del entorno y de las transacciones relevantes, el auditor debe identificar el riesgo adicional involucrado con los sistemas de información mediados por la tecnología. Es así que, previo a ejemplificar algunos de los riesgos que pueden evidenciarse en base a los tramos mencionadas en el punto 5.3.2., se considera de utilidad señalar aquellos factores que, gracias a la incorporación de tecnológica, se consideran agravantes de los riesgos. Estos agravantes deben ser tenidos en cuenta por el auditor por lo que se considera oportuno dividirlos según la clasificación de los componentes del riesgo de auditoría (CPCECABA, 2013):

a) Agravantes del riesgo inherente:
   - Falta de entendimiento por parte de mandos medios o altos, de la importancia del buen manejo de las herramientas tecnológicas repercutiendo de forma negativa y considerable en el ambiente de control.
   - Falta de comprensión de la importancia del correcto mantenimiento de las aplicaciones y programas, así como de la realización de cambios en base a las necesidades operacionales y de control.
   - Contar con una infraestructura tecnológica inadecuada de soporte a los sistemas de información que no se encuentre alineada con las necesidades operacionales, especialmente si ella resulta insuficiente.
   - Pérdida o complejidad de acceso a los movimientos o registros, análisis de cuentas y a la información en general cuando se lo requiera.

b) Agravantes del riesgo de control:
   - Confianza en los programas o aplicaciones que procesan datos de manera distorsionada, que procesan datos distorsionados o ambas situaciones a la vez posibilitando el ingreso de operaciones inexistentes, el no ingreso de operaciones existentes, el ingreso de operaciones reales por montos distintos a los originales, la repetición o duplicación de operaciones y el rechazo de operaciones por error sin que exista un reproceso o alerta que permita supervisarlos.
   - Accesos no autorizados que pueden derivar en la pérdida de datos o información, en cambios inapropiados a los mismos, en el ingreso y proceso de transacciones no autorizadas entre otras. Los riesgos pueden verse particularmente incrementados si múltiples usuarios tienen acceso indiscriminado a una misma base de datos común.

- Posibilidad de que el personal TI o del área informática posea privilegios de acceso que excedan a los necesarios para desarrollar sus tareas asignadas de administración de base de datos, programaciones y entre otros.

c) Agravantes del riesgo de detección:
   - Falta de evidencia de control en la medida en que pueda afectar la evaluación del riesgo de control.
   - Intervenciones manuales inadecuadas e imperceptibles en los elementos utilizados como evidencia para el auditor.

Al evaluar los riesgos relacionados con la tecnología, es importante que el auditor involucre el concepto de "proliferación del riesgo" que se relaciona con las propiedades aditivas que poseen los mismos. Este concepto evidencia la importancia de considerar los riesgos de una forma holística a nivel entidad y no de manera individual. Así, habiendo identificado un riesgo TI A y un riesgo TI B, independientemente de que ambos riesgos sean bajos, estos pueden dar lugar a un riesgo TI C superior a la simple suma de los riesgos TI A y B. Por ejemplo, si no se observa la existencia de procesos que controlen las actividades automáticas y a la vez, se evidencia que la totalidad de los empleados poseen accesos y permisos ilimitados, si bien ambos pueden representar riesgos considerados bajos, la suma de ambos representa la posibilidad de que muchas personas puedan hacer lo que deseen en los sistemas sin ningún control que detecte o impida dichas acciones (aprobar facturas, emitir cheques, configurar nuevas cuentas de nóminas, entre otros). En estos casos, entender la administración de los riesgos y los procesos de control es importante para lograr comprender los verdaderos riesgos existentes (Juergens, 2006).

Dicho de otra manera, debe tenerse en cuenta que la falla o inexistencia de un control puede ser individual pero siempre debe analizarse conjuntamente con otros controles que sean susceptibles de fallar al mismo tiempo. Si bien puede resultar poco probable que la falla de un control resulte en un error, el hecho de que varios controles puedan fallar al mismo tiempo puede resultar en el aumento de un riesgo considerado remoto (The Institute of Internal Auditors, 2007).

A continuación, y siguiendo lo especificado por CPCECABA (2013), se describen algunos riesgos que pueden afectar a la información y que pueden evidenciarse frente al contexto tecnológico de la organización. La descripción de estos riesgos se realiza en función de los tramos establecidos precedentemente y como complemento se ejemplifican algunas amenazas traducidas en riesgos que es posible encontrar según la clasificación y definición realizada. Estos riesgos deben ser incorporados en el análisis de los tramos definidos:

Tabla 5.4.: Riesgos de la información en contextos tecnológicos

TRAMO	DESCRIPCIÓN	AMENAZAS TRADUCIDAS EN RIESGOS
Entrada	Los riesgos a los que se encuentra sujeta la información en esta etapa están relacionados con el hecho de que no todos los datos que deban ingresarse lo hagan o que los mismos sean susceptibles de ser modificados o ingresados de manera inexacta. Estos riesgos pueden tener origen en actos intencionales o en el error humano.	* Errores de operación por parte de los usuarios como consecuencia de la falta de capacitación. * Ingreso de información incorrecta o incompleta. * Falencias de integración por fallas o ausencias de interfaces. * Accesos no autorizados. * Accesos remotos no autorizados. * Superposición de funciones incompatibles en los usuarios. Segregación inadecuada de funciones.
Almacenamiento	Los riesgos a los que se encuentra sujeta la información durante esta etapa, se relacionan con su modificación, copia no autorizada y eliminación.	* Datos históricos en formatos no compatibles con la base de datos actual. * Procedimientos deficientes para las copias de seguridad y recuperación de información. * Degradación de los soportes de las copias de seguridad. * Accesos no autorizados a las bases de datos. * Robo virtual. * Ataque destructivo. * Introducción o difusión de software malicioso.
Procesamiento	Los riesgos que pueden afectar la información durante esta etapa se relacionan con la ocurrencia de errores durante el proceso o reproceso y con su modificación y eliminación.	* Errores de procesamiento o de cálculo. * Secuencia inadecuada en la ejecución de los procesos. * Performance insuficiente de los programas de procesamiento. * Interrupciones en el procesamiento de los datos. * Falta de correspondencia entre programas fuentes y ejecutables. * Cambios no autorizados a los programas o aplicaciones. * Falencias de mantenimiento de los programas o aplicaciones.
Salida	Los riesgos que pueden afectar la información durante esta etapa se relacionan con su confidencialidad y modificación así como en la detección de errores o irregularidades que surgen como consecuencia de la lectura de los reportes, consultas o informes.	* Acceso no autorizado a la información soportada por el software base. * Difusión de información no autorizada. * Intercepción de información. * Fuga de información.

Fuente: elaboración propia.

5.3.4. Identificación de los controles implementados en base a los riesgos

Una vez comprendidos los procesos, cómo estos se llevan a cabo y los distintos riesgos que pueden aparecer a lo largo de los mismos, es importante que el auditor identifique los controles que la organización aplica para eliminarlos o mitigarlos. Según lo establecido por The Institute of Internat Auditors (2007), los controles son aquellas políticas, procedimientos, prácticas y estructuras diseñadas por la organización para proporcionar una seguridad razonable de que los objetivos se alcanzarán y que los eventos no deseados serán prevenidos o detectados y corregidos. Se debe tener presente que, en los contextos

mediados por tecnología, los controles aplicados pueden consistir en controles automáticos incluidos dentro de los propios sistemas o aplicaciones bajo análisis o bien en una combinación de estos con controles manuales. Los controles manuales pueden ser independientes de las TI, utilizar información producida por las TI, derivar de controles automáticos, limitarse al seguimiento del funcionamiento efectivo de las TI y de los controles automáticos u orientarse al tratamiento de las excepciones que puedan presentarse (IAASB, 2010).

Si bien no es de interés profundizar en los controles manuales, es importante resaltar que el auditor debe prestar especial atención a estos controles dado que si bien pueden ser complementarios o suplir algunos controles automáticos inexistentes, los mismos pueden resultar menos fiables que estos últimos dado que pueden ser más fácilmente evitados, ignorados o eludidos, pueden estar expuestos a mayor cantidad de errores y equivocaciones y porque no puede asumirse que serán aplicados de manera congruente a largo del tiempo (IAASB, 2010). Por esta razón, y según lo indicado en las entrevistas realizadas, existe una fuerte tendencia en considerar que los controles automáticos generan mayor confianza para el auditor dado que son incluidos en la propia rutina del sistema y son más difíciles de sortear que los controles manuales. Sin embargo, que los controles sean automáticos no significa que los mismos sean plenamente confiables o que se encuentren íntegramente incluidos en los procesos. El auditor debe analizarlos y tenerlos en cuenta especialmente si se trata de una primera auditoría de este tipo dentro de la organización y debe indagar si los mismos se analizan de manera periódica en caso de que desarrollen sucesivos cambios en los sistemas o aplicaciones o se implementen nuevos sistemas en su totalidad.

De esta manera, y con el objetivo de realizar una identificación de los controles implementados por la organización, se propone la división de los mismos en función de la clasificación realizada por el Marco de negocio para el gobierno y la gestión de las tecnologías de información, COBIT 4.1 (IT Governance Institute, 2007). Según este marco específico, los controles referidos a los contextos tecnológicos pueden dividirse en controles generales y en controles específicos o de aplicación.

Al identificar los controles generales (ITGC), el auditor debe centrarse en aquellos controles que poseen un alcance global dado que se encuentran aplicados a la totalidad de los componentes, procesos y datos y se encuentran relacionados con muchas aplicaciones a la vez. El objetivo de identificar estos controles consiste en que el auditor obtenga un conocimiento adecuado de cómo la organización se compromete en asegurar la operación continua de los sistemas, el apropiado desempeño e implementación de las aplicaciones en

general y la seguridad de los datos (Bellino, Wells y Hunt, 2007). Siguiendo a Bellino, et al. (2007), para identificar estos controles, el auditor debe centrarse en:

- Los controles de acceso lógico sobre toda la infraestructura tecnológica, aplicaciones y datos.
- Los controles en el ciclo de vida o desarrollo de los sistemas.
- Los controles en la gestión y administración de cambios de los programas.
- Los controles en la adquisición, desarrollo y mantenimiento de aplicaciones.
- Los controles sobre la seguridad física de la base de datos.
- Los controles sobre back up y recupero de datos.
- La segregación de funciones, entre otros.

La importancia de analizar estos controles se debe a que los mismos representan un componente crítico en las operaciones y en los controles de información financiera dado que proporcionan la base para la confianza en datos, informes, controles automatizados y otras funciones del sistema subyacentes a los procesos de negocio (Deloitte Touche Tohmatsu Limited, 2018).

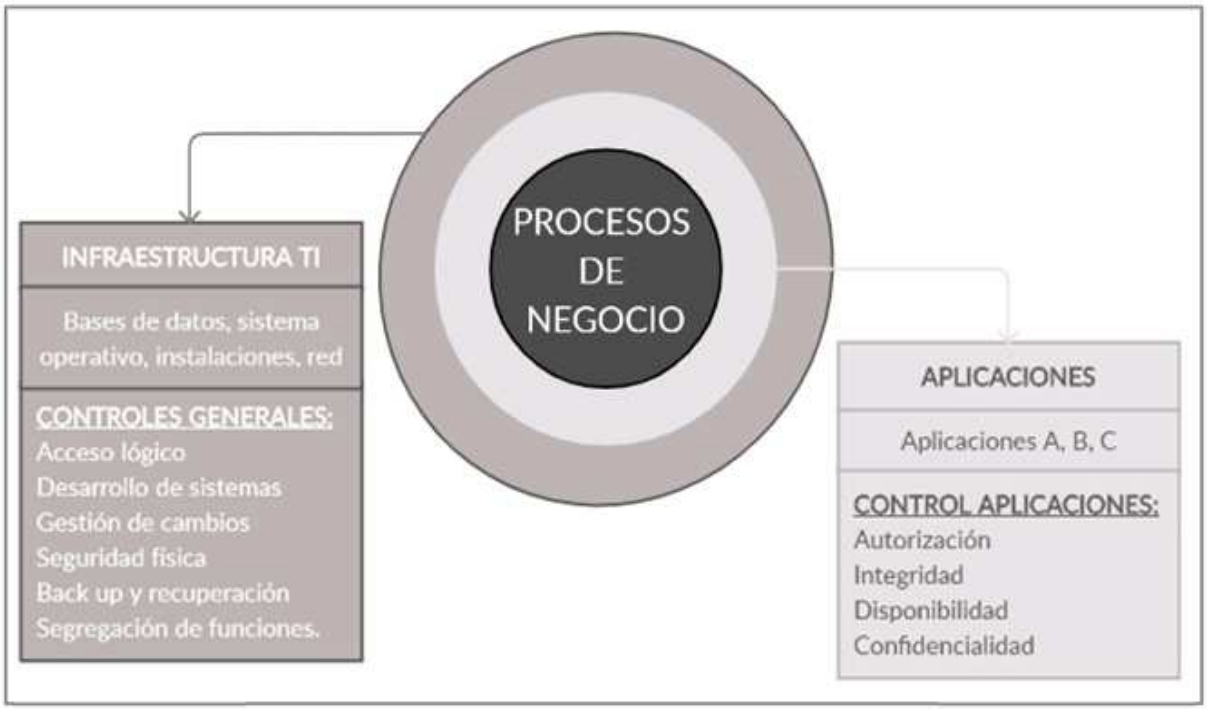
Por otro lado, y en contraposición con los controles generales, los controles de aplicación son aquellos particulares a cada uno de los sistemas o aplicaciones que se estén considerando. Al identificar estos controles, el auditor deberá centrarse en aquellos procedimientos que se encuentran en los procesos y que se diseñan para asegurar que las transacciones ocurrieron, que se encuentran autorizadas, que sean debidamente registradas, que sean procesadas de manera correcta, exacta y oportuna, que el almacenamiento sea adecuado y completo, que las salidas sean relevantes y completas, que se mantenga un registro que permita la trazabilidad del dato, entre otras (Bellino, et al., 2007). Así, CPCECABA (2013) resume estos controles en los siguientes grupos:

- Validación de datos en la entrada de las aplicaciones.
- Validación de datos en las salidas.
- Validación de interfaces entre aplicaciones.
- Validación de procesamientos de datos dentro de las aplicaciones.
- Validación de totalidad, exactitud, pertinencia, autorización, control de actualizaciones, acumulación, entre otras.

Aunque la bibliografía utilizada incluye a la segregación de funciones como un control general, resulta importante aclarar que este aspecto también tiene una influencia relevante en las aplicaciones. Si bien muchas veces su impacto no puede ser medido de forma

directa, es innegable que una inadecuada segregación de funciones puede acarrear el riesgo de errores y/o fraudes y por ello es necesario analizarla también en las aplicaciones relevantes del proceso o subproceso que se está evaluando. Adicionalmente debe contemplarse el hecho de que en aquellas bases donde la información no se encuentra integrada y se necesitan interfaces, la segregación de funciones debe ser respetada y analizada tanto en las aplicaciones de origen como en las de destino (Klus, 2018). De esta manera, cuando hacemos referencia a controles generales, la segregación de funciones se orienta al personal TI y a que las personas que están involucradas en el desarrollo y programación de sistemas estén separadas de los usuarios que ejecutaran las diversas operaciones. Mientras que, al enfocarnos en las aplicaciones, la segregación de funciones ser refiere a los accesos, permisos y privilegios que poseen los usuarios en base a los diversos perfiles (Instituto de Auditores Internos de España, 2014).

Figura 5.2.: Controles generales y de aplicación



Fuente: elaboración propia.

A continuación, y en base a CPCECABA (2013), se mencionan algunos controles a ser corroborados en base a los tramos propuestos y teniendo en cuenta los riesgos involucrados:

Tabla 5.5.: Riesgos de la información, contexto tecnológico y controles

TRAMO	DESCRIPCIÓN	AMENAZAS TRADUCIDAS EN RIESGOS	CONTROLES
Entrada	Los riesgos a los que se encuentra sujeta la información en esta etapa están relacionados con el hecho de que no todos los datos que deban ingresarse lo hagan o que los mismos sean susceptibles de ser modificados o ingresados de manera inexacta. Estos riesgos pueden tener origen en actos intencionales o en el error humano.	* Errores de operación por parte de los usuarios como consecuencia de la falta de capacitación. * Ingreso de información incorrecta o incompleta. * Falencias de integración por fallas o ausencias de interfaces. * Accesos no autorizados. * Accesos remotos no autorizados. * Superposición de funciones incompatibles en los usuarios. Segregación inadecuada de funciones.	* Seguridad lógica: Usuarios válidos. Ingreso de datos solo a través de aplicaciones válidas. Políticas de contraseña. * Seguridad física. * Segregación de funciones. * Capacitación al personal. * Ingreso completo y exacto de datos. * Rechazo de datos inexactos. * Reprocesamiento de datos rechazados. * Prevención de datos duplicados.
Almacenamiento	Los riesgos a los que se encuentra sujeta la información durante esta etapa, se relacionan con su modificación, copia no autorizada y eliminación.	* Datos históricos en formatos no compatibles con la base de datos actual. * Procedimientos deficientes para las copias de seguridad y recuperación de información. * Degradación de los soportes de las copias de seguridad. * Accesos no autorizados a las bases de datos. * Robo virtual. * Ataque destructivo. * Introducción o difusión de software malicioso.	* Protección de bases de datos por sistema operativo. * Protección de bases de datos por aplicaciones. * Antivirus. * Seguridad física. * Protección por software especializado. * Políticas de seguridad y resguardo. * Seguridad lógica del sistema operativo.
Procesamiento	Los riesgos que pueden afectar la información durante esta etapa se relacionan con la ocurrencia de errores durante el proceso o reproceso y con su modificación y eliminación.	* Errores de procesamiento o de cálculo. * Secuencia inadecuada en la ejecución de los procesos. * Performance insuficiente de los programas de procesamiento. * Interrupciones en el procesamiento de los datos. * Falta de correspondencia entre programas fuentes y ejecutables. * Cambios no autorizados a los programas o aplicaciones. * Falencias de mantenimiento de los programas o aplicaciones.	* Los procesos se ejecutan en la forma correcta. * Ningún dato es agregado, modificado o descartado en forma inadecuada durante el procesamiento. * Políticas para las modificaciones de programas o software.
Salida	Los riesgos que pueden afectar la información durante esta etapa se relacionan con su confidencialidad y modificación así como en la detección de errores o irregularidades que surgen como consecuencia de la lectura de los reportes, consultas o informes.	* Acceso no autorizado a la información soportada por el software base. * Difusión de información no autorizada. * Intercepción de información. * Fuga de información.	* Topología. * Controles criptográficos. * Seguridad de la aplicación. * Mecanismos adecuados de distribución para los datos sensibles y/o en tránsito.

Fuente: Elaboración propia.

Según lo establecido por el IAASB, 2010 y enfocándonos en los controles automáticos y en la perspectiva del auditor, los controles TI resultan eficaces cuando logran mantener la integridad de la información y la seguridad de los datos que son procesados por los sistemas de información. A pesar de que, según esta norma, estos dos factores son lo que más interesan al auditor, hay quienes consideran que la tecnología también ha afectado a otros factores representados por algunos atributos de la información y que merecen ser tenidos en cuenta gracias a que pueden dar origen a ciertos controles adicionales.

De esta forma, mientras atributos como la accesibilidad, oportunidad, y comparabilidad han sido, a rasgos generales, afectados de forma positiva por la tecnología al permitir mayor facilidad en la consulta o recuperación de datos cuando se lo necesite, en el tiempo y momento en que se lo necesite y al facilitar la posibilidad de que sean contrastados con otros, existen otros factores que merecen ser analizados con mayor grado de detalle dado que dependen del correcto establecimiento de los parámetros dentro de los sistemas y de su correcta implementación. Dentro de este grupo, según los auditores entrevistados, se incluyen a la integridad, precisión, verificabilidad, relevancia y comprensibilidad. Tomando a los atributos como un criterio de control, el auditor puede incluir dentro de su análisis, cierta tipología de controles que permitan lograr un adecuado conocimiento sobre la razonabilidad en cuanto al cumplimiento de estos requisitos de la información. De esta forma y siguiendo al Instituto de Auditores Internos de España (2020), se mencionan algunos controles adicionales que pueden ser incluidos dentro de los de aplicación y que tienen como criterio de control a algunos de los atributos mencionados.

Tabla 5.6.: Atributos como criterios y controles

Integridad	Controles de blancos, de valores inexistentes, de valores por defecto, de duplicados.
	Controles de validez relacionados con controles de formato, integridad referencial y controles de campos y/o rangos de valores tipificados.
Verificabilidad	Controles por conciliaciones de saldos, coherencia ente datos, validaciones de negocio, réplica de cálculos complejos, anclaje de información.
Disponibilidad	Controles de supervisión de procesos, controles de rechazo, totales y tendencias, controles de accesibilidad y disponibilidad.
Precisión	Controles de revisión documental o con fuentes externas reputadas y controles estadísticos de variaciones respecto a períodos anteriores.
Relevancia	Grado de conformidad de los usuarios de la información con la información recibida, revisión de las solicitudes de cambios a las aplicaciones, entre otros.

Fuente: elaboración propia en base a Instituto de Auditores Internos de España (2020).

5.3.5. Prueba y diagnóstico de controles

Identificados los riesgos y los controles que la organización implementa para mitigarlos o eliminarlos, el auditor debe elegir determinados procedimientos que le permitan proceder con la prueba de controles. El objetivo de esta prueba consiste en evaluar si los mismos son adecuados a nivel diseño, al determinar si los mecanismos planteados para mitigar los riesgos son los adecuados para cada tipo de riesgo detectado (capacidad del control para cumplir con su objetivo), a nivel implementación para determinar si el control diseñado se encuentra en uso y si se implementa tal como fue diseñado y a nivel efectividad para ver si el control funciona según lo previsto, permitiendo prevenir o mitigar el riesgo particular (CPCECABA, 2013). Para realizar la prueba de controles en función del objeto de auditoría y según lo establecido por FACPCE (2011), el auditor deberá:

- Planificar la prueba.
- Determinar el tamaño de la muestra y las cualidades que deberán poseer los elementos que serán sometidos al análisis. Estas cualidades deben incluir datos que permitan validar la hipótesis del correcto funcionamiento de los controles.
- Seleccionar la muestra, es decir el conjunto de transacciones que serán objeto de análisis para el proceso o subproceso a evaluar.
- Aplicar los procedimientos planeados.

Siguiendo el esquema sugerido, se plantea un conjunto de actividades y procedimientos para la prueba y diagnóstico de controles. A tal fin, se dividirán los controles generales de los de aplicación, siendo estos últimos segregados en función de los tramos de recolección, almacenamiento, procesamiento y salida de productos de información, mencionados con anterioridad. Para ello se han seguido a autores como Pungitore (2013), CPCECABA (2013), Rusenas (2011), Cansler (2003), Bellino, et al. (2007), Echenique García (2001), IT Governance Institute (2007 y 2012) entre otros, así como a manuales de buenas prácticas establecidos por Red Global de Conocimientos en Auditoría y Control Interno.

5.3.5.1. Controles generales

Como ha quedado expresado, a fin de enfocarse en los ITGC, el auditor debe centrarse en aquellos mecanismos que buscan garantizar una seguridad razonable de que la funcionalidad crítica TI se desarrolle de manera consistente y brinde un marco adecuado para los controles específicos al encontrarse relacionados con las funciones de quienes intervienen en las funciones TI y por constituir el medioambiente en el que se desarrollan la totalidad de los sistemas (Klus, 2018).

5.3.5.1.1. Prueba de controles generales

A continuación, se propone un conjunto de actividades y procedimientos que han sido organizados y estructurados en una guía cuyo objetivo consiste en señalar las bases que permiten optimizar la revisión y prueba de los controles mencionados.

Tabla 5.7.: Guía para la revisión y prueba de controles generales

Nro.	Actividad	Comentarios
1	Corroborar si los usuarios ingresan a la red y a las aplicaciones mediante identificación (usuario) y autenticación (contraseña) garantizando que la interacción con el sistema se haga de manera controlada.	
2	Corroborar si existen políticas de accesos y permisos de forma que el personal se encuentre autorizado dentro del cumplimiento de sus cargos, funciones y no otras, a fin de proteger la información y los recursos de actividades fraudulentas o errores.	
3	Verificar que existan, a rasgos generales, tres niveles de permisos: primer nivel donde se puedan hacer únicamente consultas, segundo nivel donde se pueda hacer captura de datos, modificaciones y consultas y tercer nivel donde se permita, además de todo lo anterior, realizar bajas.	
4	Verificar la existencia de procedimientos formales para la emisión y mantenimiento de contraseñas e indagar si se cumplen. Verificar si dichas políticas contienen como mínimo las siguientes pautas: que exista por cada usuario una contraseña única para ingresar a la red y otra para las aplicaciones, que se encuentren inhabilitadas las opciones de recordar contraseñas, que las mismas se cambien de manera periódica y bajo requerimientos automáticos, que cumplan con una longitud determinada y posean una combinación de caracteres seguros, que se recuerde al personal que las mismas no deben enviarse por correo electrónico o escribirse en papeles, que no se utilicen datos personales, entre otras.	
5	Verificar, a través de la revisión de listas de usuarios, que no existan usuarios genéricos ni perfiles utilizados por más de un usuario así como usuarios activos de ex empleados o personal ajeno a la organización de forma que se incremente el riesgo de accesos no autorizados.	
6	Verificar si con cada rotación de personal se asignan correctamente los nuevos accesos y permisos dejando inactivos o bloqueados los que correspondían al antiguo puesto, cargo o función.	
7	Indagar respecto a cómo son otorgados los permisos cuando ingresa nuevo personal. Verificar si se analiza la posibilidad de que este posea, desde el inicio, el mismo perfil que el empleado anterior, permitiendo que autorice o realice exactamente las mismas tareas o posea accesos mayores a los que corresponderían para quién inicia nuevas actividades.	
8	Verificar si se realizan análisis periódicos a los perfiles de usuario vinculados con cada función particular a fin de garantizar que no se hayan realizado cambios a los accesos o permisos sin la adecuada autorización de una persona de rango superior correspondiente y siguiendo la correcta estructura organizacional.	
9	Verificar si existen registros de actividades de los usuarios a fin de revisar a qué información han accedido, qué tareas han realizado, qué días y horarios, entre otros.	

Continuación

Nro.	Actividad	Comentarios
10	Verificar que se utilicen mecanismos de *auto-logout* que cierren los sistemas o aplicaciones después de un determinado tiempo de inactividad, asegurando que nadie pueda suplantar al usuario activo. Corroborar a su vez, si para los sistemas o aplicaciones es posible mantener dos o más sesiones activas para un mismo usuario.	
11	Verificar si existe un número máximo de intentos fallidos para ingresar a la red o a los sistemas, que invaliden los códigos de acceso y dé aviso al personal responsable.	
12	Entrevistar al personal TI para saber cómo se lo capacita, si se encuentra debidamente preparado para sus tareas y si se lo controla, así como los procedimientos que debe seguir cuando debe resolver alguna situación conflictiva o error.	
13	Verificar la existencia de matrices de segregación de funciones que permitan evaluar e identificar posibles conflictos en los perfiles o roles asignados.	
14	Analizar la segregación de funciones referidas al ambiente TI mínimamente en cuanto a que: el personal que ingresa o procesa datos no pueda generar ni aprobar transacciones, que no pueda realizar modificaciones a programas ni a archivos, que tenga prohibido el acceso a los programas fuente y a la documentación de los sistemas, que el personal perteneciente al área informática y que tenga acceso a los programas, no pueda ejecutar los mismos, ente otros.	
15	Analizar, como complemento al análisis de la segregación de funciones, la concentración de funciones en una misma persona de forma que no se generen fuertes situaciones de dependencia. Esto último es válido tanto para los usuarios de los sistemas como para el personal TI.	
16	Verificar aspectos relacionados con la seguridad física como por ejemplo que los accesos al centro de cómputos y servidores se encuentren restringidos por cuartos aislados, cerraduras, tarjetas de acceso u otro medio que impida accesos no autorizados, controles que protejan las bases de datos y los activos sensibles de hardware y software que almacenan la información, entre otros.	
17	Verificar si existen procedimientos definidos para la realización de back up o copias de seguridad donde se establezca como mínimo: la frecuencia con la que deben ser realizadas, si las mismas se realizan solamente sobre los datos o es para toda la información (tanto crítica como no crítica), si existen registros que permitan identificar lo que posee cada copia, si las mismas se encuentran rotuladas, cómo deben protegerse estas copias y dónde se almacenan, si se contemplan políticas para su eliminación y si existe un registro de ello, entre otras. Corroborar si dichos procedimientos se cumplen.	
18	Verificar que exista una adecuada planificación de los procesos y programas en especial cuando se utilicen sistemas altamente complejos donde se requiere de la ejecución de varios procesos para preparar la información en sucesivas y concurrentes etapas. Indagar qué pasa si no se cumple con dicha planificación.	
19	Verificar si la organización cuenta con un inventario detallado de los programas e interfaces en funcionamiento y si existen controles periódicos que los validen. Es importante verificar que los programas que se encuentren en funcionamiento sean los aprobados por la organización. Indagar además, cuál es el procedimiento para las aplicaciones fuera de funcionamiento y como se garantiza su no utilización.	
20	Corroborar si la organización mantiene actualizados sus sistemas operativos y aplicaciones críticas e indagar si se realizan controles periódicos de seguridad lógica para detectar posibles vulnerabilidades. Indagar sobre las acciones implementadas por la organización en caso de desvíos.	

Continuación

Nro.	Actividad	Comentarios
21	Verificar la existencia de documentación que respalde los cambios en los sistemas, que los mismos respondan a objetivos claros y se encuentren debidamente detallados, que se hayan evaluado en cuanto al impacto que podrían generar, que se realicen pruebas para corroborar el cumplimiento de los objetivos y que quede una debida constancia de su aprobación por los niveles adecuados y con conocimiento suficiente sobre el diseño y operación del sistema.	
22	Verificar si los cambios, una vez realizados, son revisados y probados previamente a su implementación así como la existencia de planes de capacitación técnica y operativa para los usuarios que operarán con las nuevas actualizaciones o desarrollos. Consultar si con cada cambio se revisan los procedimientos y la documentación de respaldo correspondiente.	
23	Consultar si se realizan copias de los programas sujetos a modificaciones a fin de que no interrumpan el normal uso por parte de los usuarios y permitiendo que puedan ser utilizados como prueba y de forma separada para verificar la eficacia de las actualizaciones o mejoras.	
24	Verificar la existencia de controles destinados a asegurar que los programas no sean fácilmente accesibles para su modificación o ejecución parcial.	
25	Para aquellos casos donde haya sido necesario contratar a proveedores externos para los nuevos desarrollos o cambios, verificar la existencia de contratos donde se especifique el objeto, alcance, cronogramas, entregables, seguimientos, honoraros, pólizas de garantía, políticas de seguridad de la información, confidencialidad y privacidad, plan de continuidad, plan de capacitación para los usuarios, entre otros.	
26	Verificar si existen *logs* de auditoria (*audit trail*) que permitan la trazabilidad de los cambios realizados a las aplicaciones y el rastreo de los responsables (usuarios o funcionarios), fechas, hora y tipo de modificaciones realizadas a los sistemas, así como la posibilidad de realizar modificaciones a la propia bitácora o log de auditoría del sistema.	
27	Verificar si la base de datos se encuentra protegida por el sistema operativo o por algún software o aplicación específicos de seguridad así como la existencia de un sistema de antivirus actualizado que proteja a los servidores donde reside la base de datos, a la red y a las estaciones desde donde se realizan las conexiones a dicha base.	
28	Verificar la existencia y cumplimiento de políticas respecto a la distribución de la información, al encriptado de la archivos tanto mientras esperan ser transmitidos como durante la transmisión y recepción, si se permite extraer información de los equipos por dispositivos externos como *pen drives* o memorias *USB*, entre otros.	
29	Verificar si se cuenta con limitaciones en el acceso remoto a los equipos y dispositivos móviles y que las conexiones remotas a la red corporativa se realicen a través de canales seguros como las *VPN*. Verificar si existen adecuados parámetros que impidan la conexión a través de redes inalámbricas inseguras.	

Fuente: elaboración propia.

5.3.5.1.2. Diagnóstico de controles generales

Como quedó expresado con anterioridad, es de esperar que los controles generales cubran (casi) la totalidad de las aplicaciones utilizadas por la organización, por ello resulta necesario

que el auditor realice un análisis integral de los mismos. Según The Institute of Internal Auditors (2007), uno de los principios básicos a ser considerados consiste en entender que la mitigación de los riesgos a través de los controles generales no se logrará a través de controles individuales sino más bien a través del conjunto de controles. Estos controles generales no se relacionan de manera directa con los riesgos de errores materiales en la información o en las declaraciones sino más bien con la seguridad razonable de que la funcionalidad crítica de TI se desarrolle de manera consistente y brinde un marco adecuado para los controles específicos o de aplicación.

El auditor debe tener en cuenta que, en muchos casos, un problema en los controles generales puede invalidar al conjunto de controles de aplicación dado que los primeros son vistos como un marco de control para los segundos. Los controles generales son habitualmente más sencillos de probar que los controles específicos o de aplicación y si fallan, el auditor puede concluir que el control interno del sistema de información es desfavorable aún sin la necesidad de llevar a cabo pruebas adicionales sobre los controles específicos. Por el contrario, y en general, el auditor solo podrá llegar a la conclusión de que el control interno del sistema de información es favorable en cuanto a la mitigación de los riesgos, si los controles generales funcionan de manera adecuada y se obtiene evidencia sobre la implementación y funcionamiento apropiado de los controles de aplicación (CPCECABA, 2013 y Cansler, 2003).

En otras palabras, sin la evaluación de los ITGC el auditor no puede concluir que estos funcionan de manera uniforme y efectiva porque cualquier persona podría modificar la configuración de un sistema en cualquier momento o podría estar accediendo a la base de datos utilizada por la aplicación. Por ejemplo, por más que no sea posible modificar una nómina a través de una aplicación, los cambios se podrían estar realizando directamente sobre las tablas que contienen la información, arribando al mismo resultado deseado por quien tiene intenciones de realizar la manipulación (Klus, 2018).

A raíz de ello, para la evaluación de estos controles se propone realizar un diagnóstico en base a un conjunto de aspectos claves que representan puntos focales de control, de los cuales es posible desprender determinados factores de riesgo que se encuentran representados por las diversas situaciones adversas que pueden presentarse como consecuencia de la falta o inexistencia de controles o de la aplicación de controles inadecuados. De esta forma, en base a la guía propuesta en el apartado anterior, que tiene como objetivo la prueba de los controles existentes y la identificación de aquellos controles inexistentes, se propone la valoración de la presencia del factor de riesgo teniendo en cuenta las siguientes situaciones: a) ausencia de controles que deberían ser

implementados, b) existencia de controles pero siendo los mismos inadecuados o incompletos, c) existencia de controles, adecuados y completos pero que no funcionan totalmente según lo previsto, d) existencia de controles eficaces y e) escasa seguridad o supervisión de controles. Como resultado de estas alternativas y en base a la siguiente escala propuesta, el auditor deberá aplicar su criterio para identificar cuándo los diversos factores de riesgo se presentan y en qué medida.

	CLASIFICACIÓN DEL RIESGO		
El riesgo es	**ALTO**	**MEDIO**	**BAJO**
Si la respuesta es	Si	A veces	No
Por lo que se le otorga una valoración de	3	2	1

De la aplicación de dicha escala a la presencia (o ausencia) de los distintos factores de riesgo posibles, el auditor puede arribar a una conclusión en función de la valoración total obtenida. Dicha valoración total del riesgo se obtiene a través del promedio simple de la valoración individual de cada factor de riesgo, teniendo estos una asignación equitativa de peso relativo en la identificación del riesgo correspondiente. De esta forma, y en base a la valoración total resultante, el auditor puede arribar a las siguientes conclusiones:

Tabla 5.8.: Tabla de resultados de controles generales

Promedio	Consecuencia
De 1,000 a 1,300	Los controles generales otorgan un marco fuerte para los controles específicos o de aplicación. Se recomienda continuar con el seguimiento de los controles establecidos para que la efectividad de estos mitiguen todo riesgo existente posible.
De 1,301 a 2,000	Los controles generales otorgan un marco aceptable para los controles específicos o de aplicación pero se debe continuar con su implementación y fortalecimiento a fin de gestionar de mejor manera los riesgos que pueden afectar a la infomación.
De 2,001 a 3,000	Los controles generales otorgan un marco deficiente para los controles específicos o de aplicación. Se requiere de la implementacion de nuevos controles que mitiguen los riesgos que pueden afectar a la información.

Fuente: elaboración propia.

Es importante aclarar que tanto los aspectos claves como los factores de riesgo incluidos en el siguiente cuadro de diagnóstico, constituyen meros ejemplos de las situaciones a ser consideradas por el auditor y no pretenden constituir una lista taxativa. Podrán realizarse adiciones o sustracciones en función a las características de la organización objeto de auditoría o al criterio profesional del auditor.

Tabla 5.9: Diagnóstico de controles generales

DIAGNÓSTICO DE LOS CONTROLES GENERALES								
ASPECTO CLAVE	**FACTOR DE RIESGO**	**PRESENCIA DEL FACTOR DE RIESGO**				**VALORACIÓN**	**OBSERVAC.**
		NO	**A VECES**	**SI**	**N/A**		
La organización cuenta con adecuadas medidas de control y análisis de los **accesos** otorgados.	Ausencia de supervisiones respecto a los ingresos a la red y a las aplicaciones.						
	Ausencia de un inventario actualizado de los accesos otorgados.						
	Accesos otorgados sin evaluar la adecuada segregación de funciones o que no se corresponden con las funciones o perfiles correspondientes.						
	Ausencia de seguimiento a los accesos frente a cambios o rotación del personal.						
	Ausencia de supervisión y actualización de los accesos otorgados.						
	Ausencia de mecanismos de *auto-logout* que impidan que las sesiones se mantengan activas frente a un determinado tiempo de inactividad así como de mecanismos que impidan mantener dos o mas sesiones activas para un mismo usuario.						
	Inexistencia de mecanismos de bloqueo frente a sucesivos intentos fallidos de acceso.						
La organización posee adecuadas medidas tendientes a la buena administración de **usuarios y contraseñas**.	Ausencia de políticas de creación y mantenimiento de contraseñas que permitan alcanzar niveles adecuados de seguridad.						
	Existencia de usuarios y/o contraseñas compartidos o genéricos.						
	Existencia de usuarios activos para ex empleados o terceros.						
	Inexistencia de supervisiones periódicas a los permisos asignados.						

Continuación

DIAGNÓSTICO DE LOS CONTROLES GENERALES							
ASPECTO CLAVE	FACTOR DE RIESGO	PRESENCIA DEL FACTOR DE RIESGO				VALORACIÓN	OBSERVAC.
		NO	A VECES	SI	N/A		
Cada usuario posee, para cada acceso, un determinado nivel de **permisos** que son otorgados en base a su responsabilidad y funciones.	Permisos otorgados sin evaluar la adecuada segregación de funciones o que no se corresponden con las funciones o perfiles correspondientes.						
	Ausencia de distintos niveles de permisos que garanticen el desarrollo de actividades en base a lo autorizado y que impidan, entre otros aspectos, la posibilidad de borrar o eliminar datos de manera indiscriminada.						
	Ausencia de seguimiento a los permisos frente a cambios o rotación del personal.						
	Ausencia de registros de actividades que permitan controlar lo realizado, consultado y modificado por los empleados en base a sus permisos.						
	Las modificaciones en los permisos se realizan sin ser autorizadas por un nivel apropiado en la organización.						
Todo **sistema o aplicación** utilizado es controlado y monitoreado por un área o responsable específico encargado de identificar desviaciones e irregularidades, así como sus cambios o	Ausencia de una adecuada planificación de los programas objeto de desarrollo.						
	Inexistencia de un inventario actualizado de programas e interfaces en funcionamiento y debidamente aprobados, así como de mecanismos que inhabiliten el uso de los que se encuentran fuera de funcionamiento.						
	Ausencia de actualizaciones periódicas a los sistemas operativos y aplicaciones críticas.						
	Ausencia de documentación que respalde los cambios solicitados a los programas y que contengan detalles, justificaciones y autorizaciones correspondientes.						
	Ausencia de revisiones y aprobaciones antes de la implementación de los cambios realizados.						
	Ausencia de copia de programas para la realización de pruebas de cambios y que permitan el normal funcionamiento de los mismos.						

Continuación

DIAGNÓSTICO DE LOS CONTROLES GENERALES							
ASPECTO CLAVE	**FACTOR DE RIESGO**	**PRESENCIA DEL FACTOR DE RIESGO**				**VALORACIÓN**	**OBSERVAC.**
		NO	**A VECES**	**SI**	**N/A**		
modificaciones respectivas.	Ausencia de *logs* de auditoría que permitan la trazabilidad de los cambios (*audit trail*).						
	Ausencia de capacitaciones técnicas al usuario frente a las modificaciones de los programas que utiliza y de actualización a los manuales de procedimiento correspondientes (en caso de existir).						
	Ausencia de acuerdos y detalles formales frente a la incorporación de proveedores externos.						
Todo **hardware** utilizado es controlado y monitoreado por un área o responsable específico encargado de identificar desviaciones e irregularidades.	Ausencia de políticas adecuadas de seguridad física orientadas a la protección de los activos informáticos contra daños y a la adecuada configuración de seguridad de los mismos.						
	Inexistencia de inventarios actualizados de todos los dispositivos hardware y del personal a cargo de su utilización, así como de su adecuada identificación a través de códigos unívocos y de un correcto seguimiento de los mismos.						
	Ausencia de políticas y procedimientos adecuados para la baja de los activos de forma que incrementan el riesgo de pérdida de información.						
	Ausencia de políticas de seguimiento adecuadas para los dispositivos hardware clasificados como críticos para la continuidad del negocio.						
	Dispositivos hardware conectados a la red sin autorización.						
	Los empleados pueden disponer de la información de la organización de manera libre y sin ningún control.						
	Ausencia de inventario de información clasificada y de matrices de clasificación de acuerdo a la criticidad y al riesgo que presenta la información.						
	Ausencia de supervisión frente al uso de archivos sensibles.						

Continuación

DIAGNÓSTICO DE LOS CONTROLES GENERALES								
ASPECTO CLAVE	**FACTOR DE RIESGO**	**PRESENCIA DEL FACTOR DE RIESGO**				**VALORACIÓN**	**OBSERVAC.**
		NO	**A VECES**	**SI**	**N/A**		
La organización aplica políticas, diagnósticos y chequeos que le permitan **asegurar, resguardar y proteger** la información.	Ausencia de aplicaciones específicas de seguridad para la protección de la información, así como de sistemas de antivirus actualizados que protejan los servidores.						
	Debilidades en el procedimiento para la realización de las copias de seguridad.						
	Frecuencia inadecuada en la realización de las copias de seguridad para los niveles de actividad.						
	Ausencia de políticas de eliminación y retención de la información.						
	Inexistencia de adecuados mecanismos de cifrado para datos, archivos o registros.						
	Se permite extraer información de los equipos por dispositivos externos como *pen drives* o memorias *USB*.						
	No se cuenta con limitaciones en el acceso remoto a los equipos y dispositivos móviles, de forma que, en caso de perdida o robo, puedan ser bloqueados y no se permita a terceros el acceso a la información.						
	Ausencia de políticas de confidencialidad.						
	Limitada formación de los empleados en controles de seguridad para la administración de la información.						
	Ausencia de un plan de formación continuo en ciberseguridad y de planes de respuesta frente a la violación de los datos.						
	Ausencia de un inventario de eventos que alertan de potenciales ataques externos y de sus correspondientes planes de acción para su mitigación.						

Fuente: elaboración propia.

Siguiendo la metodología propuesta, una vez realizadas las pruebas necesarias sobre la dimensión de controles generales y luego de haber concluido sobre el nivel de confianza de los mismos, podremos continuar con la prueba de controles de las aplicaciones relevantes que soportan la gestión de los procesos o subprocesos incluidos en el alcance del trabajo de auditoría.

5.3.5.2. Controles de aplicación

Así como los controles generales buscan garantizar una seguridad razonable de que la funcionalidad crítica de TI se desarrolle de manera consistente y brinde un marco adecuado para los controles específicos, estos últimos revisten otro grado de importancia dado que toda la información es generada y soportada por las diversas aplicaciones. De esta manera, los controles específicos buscan garantizar que las aplicaciones se ejecuten con la frecuencia necesaria, utilizando los archivos fuente actualizados, procesando la totalidad de las entradas, entre otros controles enunciados a continuación (The Institute of Internal Auditors, 2007).

5.3.5.2.1. Prueba de controles específicos

De la misma manera que lo desarrollado para los controles generales, a continuación, se propone un conjunto de actividades y procedimientos que han sido organizados y estructurados en una guía, cuyo objetivo consiste en señalar bases que permiten optimizar la revisión y prueba de controles de aplicación en base a los tramos previamente mencionados. Para ello se ha tomado como referencia lo enunciado por autores como Pungitore (2013), CPCECABA (2013), Rusenas (2011), Cansler (2003), Bellino, et al. (2007), IT Governance Institute (2007 y 2012) entre otros, así como lo establecido en manuales de buenas prácticas de Red Global de Conocimientos en Auditoría y Control Interno.

5.3.5.2.1.1. Tramo: Recolección de elementos de entrada

Como se expresó anteriormente, en el proceso de recolección de elementos de entrada, los riesgos que sufre la información están relacionados a con su integridad y exactitud de forma que no todos los datos que deban ingresarse lo hagan o que los mismos sean susceptibles de ser modificados o ingresados de manera inexacta ya sea por exceso o por defecto. El origen de este tipo de riesgos puede estar relacionado con actos intencionales o con el propio error humano (CPCECABA, 2013).

El análisis del proceso de entrada de datos posee una característica particular dado que constituye la primera etapa en el proceso de generación de información y es, sin dudas, una de las que mayor importancia reviste dado que un exceso o defecto en los datos de entrada, campos incompletos, información duplicada o una carga fuera de rango de tiempo necesario afectarán a los tramos subsiguientes de procesamiento, almacenamiento y salida de información. No por casualidad representa una de los tramos que mayores revisiones necesita a la hora de evaluar los riesgos y controles y, al igual que para el resto de los mismos, requiere de una persona responsable del control de esta información y que asegure que la misma sea confiable y oportuna (Echenique García, 2001).

En este tramo se busca evaluar la manera en que se llevan a cabo las acciones de recopilación y captura de datos necesarios para iniciar el procesamiento de transacciones. Las entradas pueden realizarse de manera manual, por ejemplo, al realizar la carga de una factura a ser abonada, o de manera automática mediante dispositivos especiales como el proceso de archivos por lotes o la lectura a través de los códigos de barras. El auditor debe tener presente que mientras mayor sea la captura de datos directa de su fuente con un mínimo de esfuerzo manual, más seguridad se tiene respecto a que el registro o archivo se realice con precisión y en forma oportuna. De forma contraria, a mayor cantidad de actividades manuales, mayores riesgos de cometer errores y menor seguridad en cuando a la precisión y oportunidad (Perfumo, 2013).

Tabla 5.10.: Guía para la revisión y prueba de controles específicos. Recolección

Nro.	Actividad	Comentarios
1	Verificar que las transacciones sean adecuadamente autorizadas antes de ser procesadas informáticamente. Las autorizaciones podrán depender del nivel de riesgo de la transacción o bien de los controles propios donde opera la misma.	
2	Enumerar las transacciones críticas objeto de la revisión, ya sean manuales o automatizadas, identificar quiénes las realizan y verificar la existencia de adecuados controles cruzados que permitan detectar inconsistencias o errores.	
3	Validar que el ingreso de los datos se haga solo a través de aplicaciones válidas y vigentes y no por otros medios como programas utilitarios que accedan a la base de datos directamente.	
4	Verificar que las entradas manuales de datos se realicen o crucen a través de algún documento físico u otro soporte que respalde la transacción. Adicionalmente, si estos documentos son internos, verificar que se trate de documentos de origen prenumerados de forma que se facilite su registro y control de su posterior procesamiento.	
5	Verificar que, en aquellos casos donde se evidencie la anulación o extravío de los documentos de origen, se encuentre una adecuada justificación ingresada y registrada en el sistema a fin de evitar que se procesen operaciones no autorizadas bajo sus números identificatorios.	

Continuación

Nro.	Actividad	Comentarios
6	Verificar que, para el caso del procesamiento en lote, se encuentre un detalle de la cantidad de documentos que este contiene, de la denominación de los documentos a ser procesados, una enumeración de la transacción inicial y final en él contenidas y controles de totales. Corroborar que se realicen reconciliaciones periódicas teniendo en cuenta los saldos iniciales y finales a fin de identificar perdida de datos, adiciones o errores diversos.	
7	Verificar si el ingreso de datos se realiza siguiendo determinados parámetros específicos ya establecidos en los sistemas a fin de minimizar errores.	
8	Verificar si el sistema permite continuar con las actividades o tareas a pesar de que no se haya ingresado la totalidad de los datos requeridos para cada transacción particular (controles de blancos).	
9	Verificar si el sistema permite el ingreso de datos que no se correspondan con los datos o rangos esperados y verificar que la aplicación los rechace a través de controles de consistencia.	
10	Verificar la anexión de algún código particular a ciertas transacciones de entrada (como número de expediente, número de trámite, ticket, entre otros) que permita seguir dicho elemento de entrada en cualquier etapa de su procesamiento, verificación de resultados, entre otros permitiendo así su trazabilidad.	
11	Verificar que existan comprobaciones de secuencia numérica que faciliten la trazabilidad de las transacciones y que permitan controlar la integridad de los datos ingresados.	
12	Verificar que las transacciones incorrectas sean rechazadas y se dé aviso en el momento de la carga. Verificar si el sistema tiene previsto el almacenamiento de la información rechazada y cómo el usuario verifica que no se genere su pérdida.	
13	Verificar si la aplicación genera un registro de datos rechazados o en suspenso y corroborar los procedimientos para su corrección, reproceso o eliminación y la forma en que los usuarios los revisan. Se debe corroborar que la no admisión de las transacciones quede documentada y grabada en el sistema hasta tanto se corrija la causa que generó el rechazo, situación que, una vez solventada, permita el reingreso al sistema sin más inconvenientes.	
14	Verificar, en base al punto anterior, si el sistema contiene mecanismos que comuniquen a los usuarios cuándo los datos o transacciones rechazados superan una antigüedad determinada o excedan una determinada fecha de corte.	
15	Verificar si el sistema permite la doble digitación de los campos críticos a fin de que se impida su registro incorrecto. En caso de producirse un error, corroborar que el sistema alerte al usuario sobre la inconsistencia en los valores cargados.	
16	Verificar si, para aquellos casos donde no se admite la duplicación de alguna carga, la aplicación rechaza su entrada al intentar reingresarla nuevamente.	
17	Verificar que los caracteres admitidos en cada campo sean los que corresponden y que no se evidencien caracteres numéricos donde deban existir letras o símbolos o viceversa.	

Continuación

Nro.	Actividad	Comentarios
18	Verificar, frente a la existencia de datos fijos, que los ingresos sean realizados de manera correcta e íntegra según las necesidades transaccionales. Si bien la responsabilidad final del control sobre los datos fijos es del usuario, es aconsejable corroborar que el sistema permita controlar dichos datos vigentes sobre todo cuando las actualizaciones requieren nuevos ingresos de manera recurrente.	
19	Corroborar que las altas de estos datos fijos se encuentren acompañadas de las autorizaciones correspondientes.	
20	Verificar si, para aquellos casos donde los registros derivados requieren de la existencia de un registro previo, puede cargarse algún ingreso sin que exista algún dato previamente incluido en la base de datos.	
21	Verificar los controles existentes en las interfaces entre aplicaciones cuando el sistema no sea de tipo integrado. Indagar cómo el área de sistemas o encargado correspondiente realiza la transmisión de un medio a otro y qué mecanismos de control aplica para garantizar que el proceso de transferencia de datos sea completo, preciso, oportuno y no presente duplicaciones.	
22	Verificar si los procesos de interface poseen controles que permitan verificar la autenticidad del origen.	
23	Verificar que el procedimiento de interface contemple la recuperación de información en caso de interrupción del proceso o de encontrarse inconsistencias. Corroborar que el sistema permita el control de errores de interfaces para su revisión y ajuste.	

Fuente: elaboración propia.

5.3.5.2.1.2. Tramo: Procesamiento de datos en información

En este tramo, el auditor debe basar su análisis teniendo en cuenta que los riesgos a los que se encuentra sujeta la información durante el procesamiento se relacionan con su eliminación, modificación y con la ocurrencia de errores durante el proceso propiamente dicho. El control sobre el procesamiento tiene como objetivo asegurar que el mismo es completo, preciso y autorizado y al igual que lo que sucede para el tramo de recolección, este también requiere un responsable que asegure que los datos recolectados sean completa y correctamente procesados (CPCECABA, 2013 y Echenique García, 2001).

Tabla 5.11.: Guía para la revisión y prueba de controles específicos. Procesamiento

Nro.	Actividad	Comentarios
1	Verificar el cálculo de los procesos más importantes y la correcta secuencia de los mismos a través de procesos como simulaciones, operaciones en paralelo o evaluación con datos de prueba. Auditar, en caso de existir, las decisiones automatizadas hechas por los algoritmos.	

Continuación

Nro.	Actividad	Comentarios
2	Comprobar si la aplicación tiene incorporados controles de totalidad o de exactitud aritmética de los registros así como la existencia de mantenimiento y revisión de registros, cuentas o balances de comprobación a fin de garantizar la coherencia de los archivos de la misma aplicación.	
3	Comprobar si la aplicación tiene incorporados controles de alertas por rechazo o cancelaciones en el proceso propiamente dicho.	
4	Revisar cómo los usuarios detectan errores o fallas en el procesamiento e indagar cómo las transacciones que presentaron estas fallas son nuevamente procesadas.	
5	Verificar que la existencia de transacciones erróneas no interrumpa el procesamiento de las transacciones válidas. Indagar qué mecanismos se utilizan para controlar dicha situación.	
6	Corroborar que ningún dato sea agregado, modificado o descartado en forma inadecuada durante el procesamiento por el mismo sistema. Analizar los saldos de apertura del período de corte actual con los saldos de cierre del período de corte anterior a través de la ecuación saldo inicial +/- movimientos = saldo final y a través de la sumatoria de saldos individuales = saldo de los registros al cierre del período de corte, entre otros.	
7	Verificar si existen controles de pruebas cruzadas como por ejemplo sumas cruzadas, donde se realizan sumas de los mismos ítems o datos desde distintas fuentes.	

Fuente: elaboración propia.

5.3.5.2.1.3. Tramo: Almacenamiento de datos

Al analizar el tramo de almacenamiento, el auditor debe tener presente que los riesgos a los que está sujeta la información durante el almacenamiento se relacionan con su eliminación, modificación y copia no autorizada (CPCECABA, 2013).

Tabla 5.12: Guía para la revisión y prueba de controles específicos. Almacenamiento

Nro.	Actividad	Comentarios
1	Verificar que a la base de datos solamente se puede acceder a través de aplicaciones vigentes.	
2	Analizar el procedimiento para la eliminación o baja de registros, del correcto ingreso de justificaciones, así como la imposibilidad de que cualquier persona pueda realizarla.	
3	Verificar si pueden realizarse modificaciones a los datos incluidos en circuitos ya cerrados.	
4	Verificar si pueden realizarse modificaciones manuales a algo liquidado o cargado de manera automática sin que existan mecanismos que permitan su revisión en una instancia posterior.	
5	Verificar que la posibilidad de modificar campos de registros ya cargados se encuentre restringida sólo al personal debidamente autorizado.	

Continuación

Nro.	Actividad	Comentarios
6	Corroborar que la posibilidad de editar o corregir un dato pueda realizarse tan cerca del punto de origen como sea posible.	
7	Verificar la existencia de mecanismos que permitan recuperar los datos cargados a lo largo del tiempo en aquellas bases vivas y donde deben realizarse cambios de manera constante, corroborando que los datos históricos no se pisen con los datos actuales.	
8	Verificar la existencia de mecanismos adecuados para el resguardo de archivos fuente y de datos dentro del propio sistema.	
9	Verificar los procedimientos de back up del software o aplicación particular. Revisar si los mismos se realizan sobre los datos y/o la información y su periodicidad. No basta con validar la existencia de procedimientos para la recuperación de la información sino que también es necesario que sean probados para garantizar el correcto cumplimiento.	

Fuente: elaboración propia.

5.3.5.2.1.4. Tramo: Salida de productos de información

Cuando se analiza una aplicación, es muy común centrar la atención en el ingreso de los datos, en su procesamiento, su retroalimentación y su almacenamiento dejando de lado aquello que da origen y constituye el inicio del sistema y que se encuentra representado por el seguimiento administrativo, la obtención de los reportes y las salidas de información (Echenique García, 2001).

Adicionalmente, cuando hablamos de salidas de información, constituye una práctica normal pensar en reportes o informes a ser utilizados para realizar análisis de ventas, compras, consumos, entre otros perdiendo de vista que el mismo puede constituir un informe o reporte clave del cual derivan otras actividades como las de control. Por ejemplo, un error no detectado en un informe o reporte de salida podría resultar en un error material si la información contenida en él se utiliza para generar una transacción como un asiento diario, se la utiliza como base de un control o bien porque ese informe es sometido a un control manual que podría no detectar el error (The Institute of Interna Auditors, 2007).

Los riesgos a los que está sujeta la información durante este tramo se relacionan con la confidencialidad y modificación, así como en la detección de errores o irregularidades que surgen como consecuencia de la lectura de los reportes, consultas o informes. Estos controles se dirigen a identificar qué se hace con la base de datos, a comparar las salidas con las necesidades de información y a cotejar estas salidas con los ingresos o entradas (CPCECABA, 2013 y Pungitore, 2013).

Tabla 5.13.: Guía para la revisión y prueba de controles específicos. Salida

Nro.	Actividad	Comentarios
1	Indagar cómo se garantiza la integridad de los datos de salida y cómo se incluyen las salidas de datos incompleta y defectuosa. Corroborar que los ítems rechazados y en suspenso sean tenidos en cuenta.	
2	Verificar si existe algún examen particular de razonabilidad de la información de salida por parte de los mandos intermedios que permita identificar algún tipo de error.	
3	Indagar sobre la existencia de aplicaciones utilizadas para la comunicación a fin de asegurar la confidencialidad de las salidas y garantizar que lleguen solo a los usuarios legítimos, así como los controles que estas aplicaciones poseen. En caso de que estas aplicaciones no existan, verificar si la organización posee políticas respecto al uso de los mails o de los dispositivos móviles como medio de traslado de información.	
4	Verificar que los accesos a la información de salida se encuentren restringidos al personal autorizado y que exista oportunidad en la recepción de los mismos.	
5	Indagar respecto a qué tipo de informes se generan a través de las aplicaciones bajo análisis y sobre el hecho de que, frente a la imposibilidad de emitir informes a medida, se deban trabajar los reportes actuales a través de hojas de cálculo o similar, lo cual podría inducir a errores. Indagar qué tipo de controles se realizan para garantizar el correcto trabajo sobre dicha información.	
6	Verificar si existe algún procedimiento respecto al período de conservación de los listados o salidas generadas y cuál es destino final de los informes o reportes que ya no se usan.	
7	Verificar la existencia de reportes emitidos por las aplicaciones destinados al control de los propios procesos y si los mismos resultan útiles y confiables, así como la existencia de múltiples reportes que permitan validar (o no) la información. Ejemplo de los mismos podrían ser: informes periódicos para el control de datos fijos, informes o estadísticas de fallas, gestión de novedades, excepciones, informes de datos actuales e históricos, informes de modificaciones a los datos ingresados, reportes de datos rechazados o en suspenso, entre otros.	
8	Indagar si existen tratamientos especiales para el caso de salidas confidenciales como cheques, recibos de sueldo, entre otros donde se involucran datos de terceros.	

Fuente: elaboración propia.

5.3.5.2.2. Diagnóstico de controles de aplicación

Siguiendo la estructura desarrollada para los controles generales y teniendo en cuenta la misma escala de clasificación del riesgo, se propone el mismo esquema para el diagnóstico de los controles tratados en este apartado. Al igual que para los ITGC, la tabla de diagnóstico se encuentra constituida por un conjunto de aspectos calves que, en este caso, hacen referencia a los tramos de recolección de elementos de entrada, procesamiento, almacenamiento y salida de productos de información. En base a esta distinción se procede a clasificar los diversos factores de riesgo a fin de lograr la valoración de la presencia de los mismos. El auditor deberá obtener la valoración individual de cada uno de estos factores para finalmente, a través del promedio simple, obtener la valoración total de los controles de aplicación.

Tabla 5.14.: Diagnóstico de controles específicos o de aplicación

DIAGNÓSTICO DE LOS CONTROLES ESPECÍFICOS O DE APLICACIÓN								
ASPECTO CLAVE	FACTOR DE RIESGO	PRESENCIA DEL FACTOR DE RIESGO				VALORACIÓN	OBSERVAC.
		NO	A VECES	SI	N/A		
Recolección de elementos de entrada	Permisos otorgados que exceden a las funciones de ingreso de datos en base al perfil del usuario.						
	Ausencia de mecanismos tendientes a garantizar la correcta autorización de las transacciones antes de ser procesadas.						
	Inexistencia de mecanismos que permitan supervisar si el ingreso de datos se realiza a través de aplicaciones válidas y vigentes.						
	Ausencia de documentos fuente que respalden ingresos manuales o automáticos a las aplicaciones.						
	Inexistencia de leyendas o bloqueos frente a transacciones que tienen como origen documentos fuente anulados o extraviados.						
	Ausencia de controles y mecanismos de identificación para el procesamiento en lote.						
	Inexistencia de parámetros adecuados que ayuden a minimizar los errores en los ingresos manuales.						
	Ausencia de controles de blancos.						
	Ausencia de controles de consistencia.						
	Inexistencia de códigos unívocos que identifiquen a cada transacción en particular y que permitan su adecuada trazabilidad.						
	Ausencia de controles de secuencia numérica que permitan o faciliten realizar controles de integridad.						

DIAGNÓSTICO DE LOS CONTROLES ESPECÍFICOS O DE APLICACIÓN								
ASPECTO CLAVE	FACTOR DE RIESGO	PRESENCIA DEL FACTOR DE RIESGO				VALORACIÓN	OBSERVAC.
		NO	A VECES	SI	N/A		
Recolección de elementos de entrada	Inexistencia de registros de datos rechazados y de mecanismos de revisión de los mismos a fin de que se corrijan y se reprocesen.						
	Ausencia de controles de antigüedad de los datos rechazados o en suspenso.						
	Ausencia de mecanismos de doble digitación para aquellos datos considerados críticos.						
	Ausencia de mecanismos de control que impidan la duplicidad en la carga de datos o que no den aviso de la misma.						
	Ausencia de controles que impidan la carga de caracteres distintos a los admitidos en cada campo de carga.						
	Inexistencia de mecanismos de control sobre el ingreso de datos fijos y de las actividades que permitan asegurar su vigencia periódica.						
	Ausencia de mecanismos de control para la carga de registros derivados.						
	Inexistencia de adecuados controles en las interfaces que permitan garantizar la integridad, precisión, oportunidad y la no duplicidad en el proceso de transferencia de datos.						
	Inexistencia de mecanismos que permitan la recuperación de la información en caso de interrupciones o errores en los procesos de interface.						
Procesamiento de datos	Permisos otorgados que exceden a las funciones de procesamiento de datos en base al perfil del usuario.						
	Carencia de controles por parte de los usuarios en los procesos de cálculo realizados por el sistema.						

Continuación

DIAGNÓSTICO DE LOS CONTROLES ESPECÍFICOS O DE APLICACIÓN							
ASPECTO CLAVE	FACTOR DE RIESGO	PRESENCIA DEL FACTOR DE RIESGO				VALORACIÓN	OBSERVAC.
		NO	A VECES	SI	N/A		
Procesamiento de datos	Inexistencias de controles de totalidad o exactitud aritmética que permitan garantizar la coherencia de los archivos de la aplicación.						
	Ausencia de controles de alerta en caso de rechazos o cancelaciones en el procesamiento propiamente dicho.						
	Inexistencia de mecanismos que permitan garantizar que las transacciones erróneas no interrumpen el procesamiento de las transacciones válidas.						
	Ausencia de controles que adviertan la incorporación, modificación o eliminación inadecuada de los datos durante el procesamiento.						
	Ausencias de mecanismos que permitan realizar pruebas cruzadas desde distintas fuentes.						
Almacenamiento de datos	Permisos otorgados que exceden a las funciones de almacenamiento de datos en base al perfil del usuario.						
	Ausencia de supervisiones que permitan garantizar el acceso a la base de datos sólo a través de aplicaciones vigentes.						
	Inexistencia de adecuados procedimientos automáticos para la eliminación o baja de registros, así como de adecuadas justificaciones.						
	Posibilidad de realizar modificaciones a los datos incluidos en circuitos cerrados.						
	Ausencia de mecanismos que permitan la revisión de las modificaciones realizadas a los datos incluidos en la base.						
	Ausencia de mecanismos que permitan recuperar los datos a lo largo del tiempo sin que los mismos se pierdan o sean pisados por datos actuales.						

Continuación

DIAGNÓSTICO DE LOS CONTROLES ESPECÍFICOS O DE APLICACIÓN								
ASPECTO CLAVE	FACTOR DE RIESGO	PRESENCIA DEL FACTOR DE RIESGO				VALORACIÓN	OBSERVAC.
		NO	A VECES	SI	N/A		
Almacenamiento de datos	Inexistencia de mecanismos que permitan editar o corregir datos cerca del punto de origen.						
	Inexistencia de mecanismos que garanticen el adecuado resguardo de los archivos fuente y de datos.						
Salida de productos de información	Permisos otorgados que exceden a las funciones del personal no autorizado a acceder a la información.						
	Imposibilidad de garantizar de manera adecuada la integridad de los datos en los informes de salida.						
	Ausencia de adecuados exámenes de razonabilidad de la información de salida por parte de los mandos intermedios.						
	Ausencia de procedimientos adecuados de comunicación que permitan garantizar la confidencialidad y privacidad de las salidas.						
	Accesos no controlados a la información de salida.						
	Inexistencia de reportes adecuados emitidos desde las aplicaciones para cubrir las necesidades de información de los propios procesos, incluyendo la validación de la información.						
	Inexistencias de procedimientos adecuados respecto a la conservación de los informes o reportes de salida así como la definición de su destino una vez utilizados.						
	Inexistencia de tratamientos especiales para salidas particulares.						

Fuente: elaboración propia.

Tabla 5.15.: Tabla de resultados de controles específicos o de aplicación

Promedio	Consecuencia
De 1,000 a 1,300	Implementación y funcionamiento apropiado de los controles específicos o de aplicación. Se recomienda continuar con el seguimiento de los controles establecidos para que la efectividad de estos mitiguen todo riesgo existente.
De 1,301 a 2,000	Implementación y funcionamiento aceptable de los controles específicos o de aplicación, pero se debe continuar con su refuerzo y fortalecimiento a fin de gestionar de la mejor manera posible los riesgos que pueden afectar a la infomación.
De 2,001 a 3,000	Implementación y funcionamiento deficiente de los controles específicos o de aplicación. Se requiere de la incorporación de nuevos controles que mitiguen los riesgos que pueden afectar a la información.

Fuente: elaboración propia.

Como ha quedado plasmado, los contextos mediados por tecnología han evidenciado un impacto importante en los sistemas de información y en sus mecanismos de control, encontrándose la evidencia de auditoría también afectada como consecuencia de las TI. Dado que muchas veces los registros informáticos solo pueden ser corroborados a través de otra evidencia informática, el auditor debe evitar caer en la simplificación de asumir que todo lo que se encuentra intervenido por la automatización es correcto y dar por sentado que todo lo proporcionado por los sistemas mediados por la tecnología es auténtico sin acudir a otra evidencia que lo corrobore. En estos casos, la autenticidad y fiabilidad de estos registros puede ser difícil o imposible de verificar si previamente no se comprenden y verifican los controles relacionados (Minguillón, 2006).

Es importante entender que, cuanto mayor sea el entorno informático de la organización auditada, más latente debe encontrarse el escepticismo profesional siendo indispensable que el auditor guíe su actividad teniendo como pilares los siguientes cuestionamientos: a) la probabilidad de que algún documento informático sea erróneo tanto accidental como intencionalmente, b) las motivaciones, oportunidades e incentivos que pueden existir dentro de la organización para alterar los datos y registros electrónicos, c) la posibilidad de que no existan pistas de auditoría que permitan vincular la evidencia informática con el hecho transaccional que la ha generado y con los datos de entrada necesarios para su procesamiento y d) la posibilidad de que se generen cambios no autorizados en la evidencia informática después de su correcta generación (Minguillón, 2006).

Adicionalmente, y a fin de poder valorar este tipo de evidencia recopilada, el auditor debe considerar que en algunos casos no será posible disponer de documentos físicos (como

facturas de proveedores) pudiendo los mismos ser visualizados únicamente a través del sistema informático. En otros casos la entidad no podrá hacerse de documentos físicos ya sea porque dicha documentación no es generada en dicho soporte por la entidad o porque llega desde el exterior existiendo solo en formato electrónico (por ejemplo: cobranzas a través de medios de pago). Frente a ello el auditor debe comprender que la copia impresa de la información en soporte informático o la lectura de la información directamente de la pantalla de la computadora, representa solamente un formato y este no proporciona ninguna indicación del origen y autorización, ni garantiza la integridad, ni la compleción de la información. En base a lo establecido por Minguillón (2006) y a modo de concluir lo esbozado en los párrafos precedentes, mencionamos aquellas consideraciones especiales a ser tenidas en cuenta por el auditor como consecuencia de los cambios introducidos por las TI:

- Se debe tener presente que en algunos casos resulta difícil determinar el origen o procedencia de la evidencia informática si solamente se analiza el soporte informático por lo que se requerirá de la utilización de ciertos controles y técnicas de seguridad que permitan validar la autenticación y reconocimiento de la misma.
- Las alteraciones a los datos o a la información puede resultar difícil, si no imposible, de detectar mediante la simple observación o examen de la información en soporte informático dado que la misma puede ser modificada a fines de ser presentada al auditor. Una vez más, la integridad de la información depende de los controles fiables y de las técnicas de seguridad empleadas.
- La información en soporte informático por sí sola no permite observar la existencia de aprobaciones a las transacciones o procesos realizados por lo que los controles y técnicas de seguridad vuelven a recobrar importancia. Anteriormente era posible observar firmas en donde ahora solo se posee una clave o llave de acceso equivalente a una autorización, dejando únicamente un registro (en el mejor de los casos) de la llave de acceso utilizada, el lugar donde se tuvo acceso y la hora y día en que fue utilizada, siendo clave analizar la cadena completa de autorizaciones. Lo indicado también puede observarse en el caso de la utilización de la firma digital que requiere de tecnologías o programas adecuados para realizar una firma fiable y consecuentemente para revisarla.
- Respecto a la compleción o integridad, debe tenerse presente que todos los términos relevantes de una operación o transacción pueden encontrarse dispersos en diversos archivos o registros de datos, tanto físicos como informáticos, por lo que se requerirá del análisis de varios registros y controles de manera simultánea.
- Finalmente, las pistas de auditoría para la información en soporte informático pueden no estar disponibles en el momento de la auditoria y el acceso a los datos puede

encontrar complejidades. La implementación de sistemas automatizados ha provocado que la pista visible de muchas transacciones haya desaparecido físicamente transformándose en algo mucho más intangible.

De esta manera, y aunque existe una marcada tendencia en depositar mayor confianza en los controles automáticos y a considerar que los sistemas informáticos han agilizado e influenciado de manera notablemente positiva en la recopilación de información por parte del auditor, ello no necesariamente implica depositar mayor confianza en la evidencia informática dado que ello podría dar origen a un nuevo riesgo derivado: la falsa sensación de seguridad. Muchas veces, para corroborar esta evidencia, es necesario aplicar mayor cantidad de pruebas que permitan verificarla y aunque poseer un perfil de auditoría (nivel uno de permisos) dentro de los sistemas a ser auditados podría representar una gran ventaja, no siempre resulta suficiente. De las entrevistas realizadas, fue posible advertir que algunos auditores consideran que la clave no se encuentra en la confianza de los reportes emitidos por los sistemas en sí, sino en el usuario y en los terceros ajenos al proceso que pueden ser un elemento de entrada o de salida el mismo. Factores adicionales como solicitar estar presente al momento del logueo, de la emisión de determinados reportes o cuando se ingresan datos y la revisión de las cadenas de autorizaciones integradas al sistema (quién aprueba, quién emite, quién paga) representan pruebas a ser aplicadas para suplir, muchas veces, lo que no puede hacerse con la simple observación de la evidencia informática.

5.3.6. Documentar conclusiones y emisión del informe final

Finalizado el diagnóstico de controles, el auditor debe documentar las conclusiones obtenidas que servirán de base para la emisión de sus recomendaciones. Estas recomendaciones deben tener relación con los hallazgos realizados, con los riesgos identificados en la ejecución de la auditoría y deben encontrarse sujetas al dinamismo de las propias operaciones de la organización, a su estructura y procesos y deben tener como propósito la mitigación de la mayor cantidad de riesgos identificados posibles.

A continuación, se propone una estructura de informe teniendo en cuenta algunas recomendaciones realizadas por el Consejo Profesional de Ciencias Económicas de Córdoba (CPCECBA, 2015) para la emisión de informes especiales. A fin de enriquecer la propuesta, el presente modelo constituye un modelo sugerido basado en un caso de riesgo alto para el proceso de generación de información.

Informe de Auditoría sobre procesos de la información mediados por la tecnología

Señor …….. de …….
ABCD
Cuit N°: ...-……..-…
Domicilio (legal/real):

I. Introducción

Mi responsabilidad consiste en expresar una opinión sobre los procesos de generación de información del área XXX, basada en mi muestra de auditoría. Mi tarea profesional fue desarrollada de conformidad con las normas sobre informes especiales establecidas en la sección VII.C de la segunda parte de la Resolución Técnica N° 37 de la Federación Argentina de Consejos Profesionales de Ciencias Económicas (en adelante, "RT 37"), aprobadas por el Consejo Profesional de Córdoba según Resolución Nº 27/14, y consistió en la aplicación de ciertos procedimientos necesarios tendientes a evaluar la utilización de medios computarizados para el proceso de generación de información.

La RT 37 exige que cumpla los requerimientos de ética, así como que planifique y ejecute mi tarea de forma tal que me permita emitir el presente informe especial. En consecuencia, mi trabajo no constituye una auditoría o revisión de estados contables, ni otro encargo de aseguramiento. Los procedimientos detallados a continuación han sido aplicados sobre los registros y documentación que me fueron suministrados por la organización.

Una auditoría conlleva la aplicación de procedimientos tendientes a obtener elementos de juicio válidos y suficientes. Los procedimientos seleccionados dependen del juicio del auditor incluida la valoración de los riesgos significativos en los procesos auditados para lo que se tendrán en cuenta los mecanismos de control diseñados e implementados por la organización. A tal efecto considero que los elementos de juicio obtenidos proporcionan una base suficiente y adecuada para la emisión de las siguientes recomendaciones.

II. Objetivo

Auditar, considerando el efecto de las TI, el proceso de generación de información relacionado con el área de XXX, detallando los principales aspectos vinculados al mismo y

evaluando la suficiencia de los controles implantados por la organización y la razonabilidad de las salidas de los sistemas involucrados.

III. Alcance

Verificar que la interacción de los sistemas existentes proporcione información correcta y necesaria para el proceso de YYY (y/o subprocesos ZZZ) en cuanto a la generación de información gerencial, de control y de cumplimiento a las disposiciones de la normativa vigente.

Si bien se han realizado procedimientos de relevamiento, análisis y evaluación de otros procesos o áreas de la organización, solo se han llevado a cabo en función de encontrarse vinculados e involucrados con el o los procesos (y/o subprocesos) bajo análisis gracias a la tarea encomendada, por lo que no se realizaran comentarios ni recomendaciones respecto a los mismos.

El alcance del presente trabajo no ha comprendido la detección de fraudes ni la evaluación de las características técnicas de la infraestructura tecnológica utilizada por la organización, por lo que no se poseen elementos de juicio necesarios para emitir una opinión sobre la situación tecnológica de la misma.

IV. Metodología de trabajo

La tarea realizada tuvo como marco principal la metodología desarrollada por el informe COSO (Committee of Sponsoring Organizations of the Treadway Commission, 2013) procediendo con las siguientes actividades:

1) *Evaluación de los controles que hacen al ambiente de control.*
2) *Relevamiento de los procesos y subprocesos a evaluar a través de:*
    - *Entrevistas a los empleados que tengan a su cargo la realización de las distintas actividades y tareas de los procesos y subprocesos para entender la operatividad.*
    - *Inspección de documentos que respalden las actividades y los registros.*
    - *Pruebas de recorrido o walkthrough que consisten en seguir una o más transacciones desde el inicio hasta llegar al final a través de un informe o*

reporte (ya sea estados contables, financieros o informes internos).

- *Indagaciones sobre el sistema informático utilizado para la gestión de la información bajo análisis a nivel transaccional.*

3) *Identificación de los riesgos en base a los procesos y subprocesos relevados.*
4) *Identificación de los controles implementados en base a los riesgos.*
5) *Prueba y diagnóstico de los controles identificados en base a las muestras seleccionadas.*

V. Hallazgos y recomendaciones

A continuación, se exponen los principales hallazgos realizados, así como sus respectivas recomendaciones o sugerencias:

1. Controles generales

a. Observación 1: *……*
Riesgo o implicancia: *……*
Recomendaciones o sugerencias: *……*

2. Controles específicos asociados a las aplicaciones

a. Observación 1: *……*
Riesgo o implicancia: *……*
Recomendaciones o sugerencias: *……*

VI. Otras cuestiones

El presente informe se encuentra dirigido y preparado exclusivamente para el uso de la Dirección de la organización ABCD, la que podrá disponer y distribuir del mismo sin restricción alguna dentro de la propia entidad. No asumo responsabilidad en el caso de que sea utilizado o se haga referencia a él o sea distribuido con otro propósito.

Por otra parte, el presente informe se encuentra referido a los hallazgos y conclusiones

sobre el objeto de la tarea hasta la fecha indicada en el informe y no contempla la eventual ocurrencia de hechos posteriores que puedan modificar su contenido.

VII. Conclusiones

De acuerdo a las pruebas realizadas y a los resultados obtenidos, se puede concluir que el proceso YYY (y/o subproceso ZZZ) es bastante limitado y propenso a la generación de errores, generando desconfianza en los procedimientos y métodos utilizados para la generación de información.

Las observaciones mencionadas determinan un contexto de alta vulnerabilidad que impide asegurar aspectos como la exactitud, integridad y confidencialidad de la información generada por la organización, así como la oportunidad de la misma.

Lugar y fecha de emisión.

Firma y sello profesional

5.4. Etapa de consolidación

Con la culminación y emisión del informe deviene la etapa de consolidación representada por el cierre del proceso de auditoría. En este espacio final, el profesional debe comunicar las conclusiones obtenidas y plasmadas en su informe exponiendo las oportunidades de mejoras detectadas, el plan de acción a seguir por la organización y cualquier otra información adicional y complementaria que desee comunicar. Con ello queda su labor sometida a consideración y aprobación procurando de esta manera, el afianzamiento de la relación con el cliente (CPCECABA, 2013).

6. Conclusión

Con el anclaje de la tecnología en el mundo actual, existe una tendencia irreversible hacia la automatización de los procesos mediante la adopción de productos y servicios TI que dejan al alcance de cualquier organización la posibilidad de mejorar la eficiencia de sus operaciones incluida la generación de información. Frente a este panorama y ante la adopción de esta herramienta como soporte a los procesos de negocio y a los sistemas de información, los esfuerzos por adaptarse a dicho cambio deben ser equitativos no solo a través de la adopción de mecanismos de control acordes sino también a través del permanente análisis y administración del riesgo derivado correspondiente.

La información es el resultado de un continuo e ininterrumpido proceso encargado de generarla, comunicarla, exponerla y resguardarla y que se encuentra dentro de la órbita de lo que conocemos como sistemas de información. Identificado este sistema y su estrecha vinculación con el proceso de generación de información, se buscó, como primer objetivo del presente trabajo, definir al mismo a fin de identificar sus componentes y funciones principales. Gracias a ello pudo concebirse a este sistema como aquel conjunto formalizado de personas, equipos y procedimientos que, trabajando de manera integrada y coordinada, capturan datos, los transforman en información, los almacenan y los distribuyen para apoyar a las organizaciones en sus actividades operativas, administrativas, de control y a sus procesos de toma de decisiones en pos de las estrategias y objetivos organizacionales (Volpentesta, 2004).

En base a este objetivo planteado, fue posible advertir que los componentes y relaciones enmarcados dentro de estos sistemas podían encontrarse estructurados en función de las actividades y toma de decisiones o bien estar orientados a las funciones organizacionales, conformando subsistemas que abarcan diversos recursos a ser utilizados en una función o aplicación particular y que revisten características particulares según el contexto en el cual se hallen inmersos. De esta forma, y considerando el entorno y la mediación tecnológica, los recursos que pueden encontrarse dentro de un sistema de información pueden clasificarse en recursos *hardware*, *software*, humanos, de datos y de redes, los cuales se fusionarán a fin de dirigir a estos sistemas hacia el cumplimiento de sus funciones básicas de recolección de elementos de entrada, de almacenamiento de datos, de procesamiento de datos en información, de salida de productos de información y de control y supervisión de su propio desempeño (Volpentesta, 2004).

Según lo visto en el capítulo II, esta última función engloba una de las propiedades de los sistemas que se encuentra relacionada con el concepto de retroalimentación. Al igual que

cualquier sistema, el de información también contiene un proceso de supervisión o evaluación encargado de mantener su funcionamiento eficiente y teniendo en cuenta sus objetivos, encontrándose dirigido no solo a sus procesos y funciones sino también a su producto final, la información. En base a dicha función, el segundo objetivo trazado buscó analizar el rol y responsabilidad del auditor en cuanto al proceso de generación de información y a la calidad inmersa en la misma. Como complemento, fue posible acercarnos al concepto de calidad informativa y a su estrecho vínculo con la utilidad de la información y con la satisfacción de las características o cualidades de la información como ponderadores de dicha utilidad en función de los diversos intereses.

Lo desarrollado en base a este objetivo permitió comprender que el hecho de establecer garantías de calidad para cualquier práctica informativa, presupone considerar, además de la responsabilidad de quienes conforman la dirección de la organización, la responsabilidad de aquellos profesionales involucrados en el proceso de generación, gestión y control de la información incidiendo a su vez, en la calidad del sistema de información. De esta forma, en la medida en que las organizaciones sean más intensivas en el uso de la información, mayor deberá ser la importancia de los recursos de la información, más elevado deberá ser el nivel de cultura orientada a ella y consecuentemente más críticos deberán ser los procesos de auditoría destinados a los mismos (González Valiente, 2014).

Tomando como marco la actual orientación del control interno hacia la administración de los riesgos de negocio, con el tercer objetivo planteado se propuso identificar aquellos factores de riesgo que pueden afectar al proceso de generación de la información considerando el entorno tecnológico organizacional. Con dicha finalidad, y gracias a las entrevistas realizadas a diversos profesionales especializados, pudo constatarse que, aunque en el ambiente empresarial existe un consenso generalizado en concebir al riesgo derivado de la tecnología con una percepción cada vez más importante, a rasgos generales el mismo no siempre es considerado significativo. Conceptualizar a las erogaciones en tecnología como costos en vez de inversiones, los tiempos y esfuerzos requeridos para su implementación y consultoría, la falta de conocimiento o capacitación del personal frente a los posibles efectos e implicancias y el hecho de no ser considerado un riesgo de impacto directo, representan factores que pueden afectar a dicha percepción e influir en la concepción de dicho riesgo considerándolo como marginal y poco significativo.

Aunque resulta evidente que los avances tecnológicos poseen gran influencia en la disminución de algunos riesgos asociados al manejo manual de datos y de información, también insertan una nueva categoría de riesgos que no puede ser ignorada y que debe estar necesariamente alineada a los riesgos de negocio (Canetti, 2007). En base a este

tercer objetivo pudo advertirse que algunos de los riesgos derivados de la tecnología en el marco de la generación de la información, se encuentran relacionados con la posibilidad de que los datos, elemento mínimo de la información, no sean ingresados de la forma debida, que puedan ser modificados o eliminados por actos intencionales o errores de operación así como la posibilidad de que la propia información pueda ser modificada, copiada o eliminada sin la debida autorización o presentar errores e irregularidades en los reportes o salidas. Errores de operación por parte de los usuarios como consecuencia de la falta de capacitación, falencias en los procesos de interfaces, accesos no autorizados, superposición o segregación inadecuada de funciones, degradación de los soportes de seguridad, errores en los cálculos o ejecución inadecuada de los mismos y cambios no autorizados a las aplicaciones representan ejemplos de posibles amenazas traducidas en riesgos que pueden afectar a la información a lo largo de todo su proceso de generación.

Para poder evaluar este proceso específico, es un requisito fundamental para quién realizará evaluaciones de un sistema de información estar actualizado en la temática y comprender que la imposibilidad de generar planes de trabajo universales, implica reconocer que los diferentes contextos tecnológicos influyen de manera diversa en las tareas de auditoria. Es por ello que, como cuarto y último objetivo específico, se buscó definir un conjunto de pautas a ser tenidas en cuenta por el profesional, a fin de estructurar su trabajo de auditoría en contextos mediados por tecnología. Dichas pautas fueron volcadas en las siguientes etapas de trabajo:

1) Etapa de comienzo: donde el auditor deberá comprender y analizar el alcance de la tarea a realizar y la posibilidad de su cumplimento teniendo en cuenta el tiempo estipulado y los recursos disponibles, así como realizar un análisis a nivel preliminar que tendrá como propósito el conocimiento del entorno operativo y del entorno de control de la entidad a auditar.

2) Etapa de análisis e implementación: donde el auditor deberá analizar la estructura, utilización e importancia de los sistemas dentro de la organización para entender su estructura TI y el nivel de dependencia al contexto tecnológico para luego, a través del relevamiento de procesos y subprocesos objeto de evaluación, identificar los riesgos involucrados en los mismos y los diversos mecanismos implementados para mitigarlos o eliminarlos. Respecto a estos últimos, se propuso la identificación de dos tipos de controles relacionados con este contexto siendo los mismos los controles generales (ITGC) y los específicos o de aplicación. Mientras que para los generales será necesario centrarse en aquellos mecanismos que posean un alcance global por estar relacionados con el medioambiente en que se desarrollan los sistemas y por

encontrarse aplicados a la totalidad de los componentes, procesos y datos, para los controles específicos se requerirá un enfoque orientado al sistema o aplicación donde se desarrolla el proceso o subproceso evaluado propiamente dicho. Finalizada la identificación de los mismos, será necesario proceder con un diagnóstico de dichos controles para evaluarlos en cuanto a su existencia y a su correcta implementación y funcionamiento para finalmente documentar las conclusiones obtenidas que servirán de base para la emisión de las recomendaciones. Estas recomendaciones deberán tener relación con los hallazgos realizados, con los riesgos identificados en la ejecución de la auditoría y deberán encontrarse sujetas al dinamismo de las propias operaciones de la organización, a su estructura y procesos.

3) Etapa de consolidación: donde se procederá al cierre del proceso, pudiendo el auditor comunicar las conclusiones obtenidas y plasmadas en su informe, así como las oportunidades de mejora detectadas procurando, a su vez, el afianzamiento de la relación con el cliente.

Considerar que el simple hecho de incorporar tecnología a los diversos procesos que conviven en una organización, incluyendo al de generación de información, traerá soluciones automáticas a los mismos, es no dimensionar adecuadamente el impacto que realmente representan estos cambios dado que no solo se requerirá de la adecuación de los procesos sino también de los controles inmersos en ellos. Sistemas de información mediados por tecnología que adolezcan de apropiados mecanismos de control producirían información carente de objetividad y confiabilidad perdiendo por completo la razón de su existencia (Canetti, 2007).

Así, si el objetivo de una organización consiste en incorporar tecnología para obtener mejores resultados en sus procesos de negocio, es responsabilidad de todos los involucrados adaptar el ambiente operativo y de control en base al rol y especialización que cada uno posee dentro de la entidad. Frente a ello, los auditores no resultan ajenos siendo necesario que ellos también se capaciten y preparen en cuanto al uso de las nuevas tecnologías, no solo para mejorar su trabajo, sino también para comprender, evaluar y responder a los riesgos que esta conlleva e influir de manera efectiva en el proceso de generación de información.

Tomando lo expuesto como cimiento, el presente trabajo realiza un aporte metodológico en relación a un conjunto de lineamientos a ser tenidos en cuenta para una auditoría de sistemas de información mediados por tecnología. El mismo se encuentra acompañado por

el diagrama de flujo del proceso propuesto, por la descripción de algunos instrumentos de utilidad orientados a la obtención de evidencia necesaria para evaluar los riesgos involucrados y los mecanismos para su mitigación, así como por el modelo de informe propuesto, teniendo en cuenta que nuestro desafío como profesionales es contribuir al diseño y desarrollo de entornos que permitan brindar información de calidad y que resulte útil para los diversos usuarios.

En base a lo indicado en el presente apartado y al desarrollo vinculado de los temas referentes a la problemática planteada, se demuestra el cumplimiento de los objetivos propuestos al iniciar el presente trabajo final de maestría.

7. Bibliografía

Altmark, D. R. (2014). La auditoría informática: aspectos jurídicos. En E.E. Martorel (Director), *Tratado de la responsabilidad de los auditores* (1era ed.) (p. 405-738) (Tomo IV). Buenos Aires: La Ley.

Bellino, C., Wells, J. y Hunt, S. (2007). Global Technology Audit Guide (GTAG) 8. Auditing application controls. Recuperado de https://www.iiacolombia.com/resource/guias/GTAG8.pdf [2020, 23 de agosto].

Calabrese, J., Esponda, S., Pasini, A. C., Boracchia, M., y Pesado, P. (2019). Guía para evaluar calidad de datos basada en ISO/IEC 25012. *XXV Congreso Argentino de Ciencias de la Computación*. *(Universidad Nacional de Río Cuarto, Córdoba, 14 al 18 de octubre de 2019)* [2020, 29 de junio].

Camisón, C., Cruz, S., y González, T. (2006). *Gestión de la calidad* (1era ed.). Madrid: Pearson Educación.

Canetti, M. M. (2007). *Contabilidad y control. Fundamentos teóricos para la mejora de la confiabilidad de la información contable.* (Tesis doctoral. Universidad de Buenos Aires, Argentina). Recuperado de http://bibliotecadigital.econ.uba.ar/download/tesis/1501-1185_CanettiMM.pdf [2019, 12 de diciembre].

Cansler, L. (2003). *Auditoría en contextos computarizados. Guía práctica profesional.* (2da ed.). Buenos Aires: Ediciones Cooperativas.

Castro, C., y Filippi, L. (2010). Modelos matemáticos de información y comunicación, cibernética: mejorar la comunicación es el desafío de nuestro destino cultural. *Revista RE - Presentaciones: Periodismo, Comunicación y Sociedad, (6),* 145-161. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=3352643 [2020, 05 de abril].

Cathalifaud, M. A., y Osorio F. (1998). Introducción a los conceptos básicos de la teoría general de sistemas. *Cinta de Moebio, (3).* Recuperado de http://www.redalyc.org/articulo.oa?id=10100306 [2020, 08 de enero].

Coba, L. G. (2006). Análisis de la calidad informativa, primer paso hacia el cambio. *Palabra Clave. Calidad y responsabilidad en la información (1),* 29-56. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=2053231 [2020, 06 de junio].

Committee of Sponsoring Organizations of the Treadway Commission (2013). Internal Control - Integrated Framework. *Executive summary.* Recuperado de https://na.theiia.org/standards-guidance/topics/documents/executive_summary.pdf [2019, 09 de diciembre].

Consejo Profesional de Ciencias Económicas de CABA (2013). *Cuaderno profesional n° 65: Efectos de la tecnología de la información* sobre el control interno (1era ed.). Buenos Aires: Edicon Fondo Editorial Consejo.

Consejo Profesional de Ciencias Económicas de Córdoba (2015). Informe especial de contador público independiente sobre la utilización de medios computarizados de registración contable. Recuperado de https://cpcecba.org.ar/ [2020, 06 de octubre].

Deloitte Touche Tohmatsu Limited (2018). General IT controls (GITC). Risk and impact . Recuperado de https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-general-it-controls-noexp.pdf [2020, 18 de mayo].

Echenique García, J. A. (2001). *Auditoría en informática* (1era ed.). México: McGraw Hill Interamericana Editores SA.

Estupiñan Gaitán, R. (2015). *Administración de riesgos E.R.M. y la auditoría interna* (2da ed.). Bogotá: Ecoe Ediciones.

Federación Argentina de Consejos Profesionales de Ciencias Económicas (2000). Resolución Técnica N° 16. *Marco conceptual de las normas contables profesionales distintas a las referidas en la Resolución Técnica N° 26.* Buenos Aires: FACPCE.

Federación Argentina de Consejos Profesionales de Ciencias Económicas (2011). *Informe Area Auditoría N° 5 Manual de Auditoría* (1a ed.). Buenos Aires: Osmar D. Buyatti.

Federación Argentina de Consejos Profesionales de Ciencias Económicas (2013). Resolución Técnica N° 37: *Normas de auditoría, revisión, otros encargos de aseguramiento, certificación y servicios relacionados.* Buenos Aires: FACPCE.

Flórez, A., y Thomas, J. (1993). La teoría general de sistemas. *Cuadernos de geografía, (4)* 111-137. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=6581658 [2020, 25 de mayo].

Fuenzalida Contreras, R. y Ambrosio Pradel, E. (2011). Riesgo tecnológico. Su medición como prioridad para el aseguramiento del negocio. Recuperado de

https://www.auditool.org/blog/auditoria-de-ti/827-riesgo-tecnologico-su-medicion-como-prioridad-para-el-aseguramiento-del-negocio [2020, 26 de octubre].

García, M. L. V. (2006). Las auditorías de la información en las organizaciones. *Ciencias de la información, 37,* (2-3), 3-14. Recuperado de https://www.redalyc.org/articulo.oa?id=181418190001 [2020, 29 de julio].

González, I. S. (2007). Cibernética y sociedad de la información: el retorno de un sueño eterno. *Signo y Pensamiento, 26* (50)*, 84-99*. Recuperado de https://www.redalyc.org/pdf/860/86005007.pdf [2020, 12 de abril].

González Valiente, C. L. (2014). Midiendo la calidad de la información gestionada: algunas reflexiones conceptuales metodológicas. *Biblos (54),* 42-50. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=4995445 [2020, 27 de junio].

Gutiérrez Pulido, H. (2010). Calidad total y productividad (3era ed.). México: Mc Graw Hill.

Hernandez Sampieri, R. y Mendoza Torres, C. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta* (1era. ed.) México: Mc Graw Hill.

Holguín Maillard, F. (2014). Riesgo de TI en auditorias de información financiera. Recuperado de https://www.auditool.org/blog/auditoria-de-ti/813-auditor-tienes-un-riesgo-ti [2019, 23 de diciembre].

Huguet Benavent, D. (2014). *Efectos de la auditoría sobre la credibilidad de la información contable de las PYMES.* (Tesis doctoral. Universitat de Valencia, Comunidad Valenciana). Recuperado de http://roderic.uv.es/handle/10550/39065 [2019, 16 de diciembre].

Instituto de Auditores Internos de España (2014). *Cobertura del riesgo tecnológico. Hacia una auditoria interna de TI integrada.* Recuperado de https://auditoresinternos.es/uploads/media_items/f%C3%A1bricati-web.original.pdf [2020, 22 de julio].

Instituto de Auditores Internos de España (2015). *Visión 2020. Desafíos de auditoría interna en el horizonte 2020*. Recuperado de https://auditoresinternos.es/uploads/media_items/150323-visi%C3%B3n2020-auditor%C3%ADa-interna.original.pdf [2020, 22 de julio].

Instituto de Auditores Internos de España (2016). *Ciberseguridad. Una guía de supervisión.* Recuperado de https://auditoresinternos.es/uploads/media_items/ciberseguridad-10preguntas-que-un-consejero-debe-plantear.original.pdf [2020, 22 de julio].

Instituto de Auditores Internos de España (2020). *Auditoria interna del gobierno del dato*. Recuperado de https://auditoresinternos.es/uploads/media_items/lfp-f%C3%A1brica-dato-web-022020.original.pdf [2020, 22 de julio].

International Auditing and Assurance Standards Board (2010). Norma internacional de auditoría 315 (NIA 315). *Identificación y valoración de riesgos de incorrección material mediante el conocimiento de la entidad y su entorno*. IFRS Foundation. Recuperado de http://www.icac.meh.es/NIAS/NIA%20315%20p%20def.pdf [2019, 11 de diciembre].

International Accounting Standards Board (2010). *Marco conceptual para la información financiera.* IFRS Foundation. Recuperado de https://www.facpce.org.ar/NORMASWEB/index_internacional.php?c=3&sc=44 [2019, 09 de diciembre].

IT Governance Institute (2007). *COBIT 4.1.* USA: IT Governance Institute. Recuperado de https://biblioteca.info.unlp.edu.ar/uploads/docs/cobit.pdf [2020, 16 de abril].

IT Governance Institute (2012). *COBIT 5.* Un marco de negocio para el gobierno y la gestión de las TI de la empresa. USA: IT Governance Institute.

Juergens, M. (2006). Global Technology Audit Guide (GTAG) 4. Management of IT auditing. Recuperado de https://www.iiacolombia.com/resource/guias/GTAG4.pdf [2020, 23 de agosto].

Klus, J. F. (2018). ¿Cómo realizar una auditoría a los sistemas de información de una organización? Recuperado de https://www.auditool.org/blog/auditoria-de-ti/6263-como-realizar-una-auditoria-a-los-sistemas-de-informacion-de-una-organizacion-2 [2020, 22 de julio].

Lambrechts, A. J., Lourens, J. E., Millar, P. B. y Sparks, D. E. (2011). Global Technology Audit Guide (GTAG) 16. Data analysis technologies. Recuperado de https://www.iia.nl/SiteFiles/IIA_leden/GTAG%2016%20Data%20Analysis%20Technologies.pdf [2020, 23 de agosto].

Lardent, A. R. (2001). *Sistemas de información para la gestión empresaria, procedimientos, seguridad y auditoría* (1ª ed.). Buenos Aires: Pearson Education SA.

Laudon, K. C. y Laudon, J. P. (1996). *Administración de los sistemas de información: Organización y tecnología* (3era ed.). México: Prentice Hall Hispanoamericana SA.

MCCafferty, J. (2017). Un día en la vida de un auditor de TI. Recuperado de https://misti.com/internal-audit-insights/a-day-in-the-life-of-an-it-auditor [2020, 31 de julio].

Minguillón, R. A. (2006). La fiscalización en entornos informatizados. *Auditoría Pública* (40) 117-128. Recuperado de https://asocex.es/wp-content/uploads/PDF/200612_40_117.pdf [2019, 24 de diciembre].

Montero, I. y León, O. (2007). A guide form naming research studies in psycology. *International Journal of Clinical and Health Psychology, 7 (3), 847-862.* Recuperado de https://www.redalyc.org/pdf/337/33770318.pdf [2020, 20 de agosto].

Navarro, J. (2001). *Las organizaciones como sistemas abiertos alejados del equilibrio* (Tesis doctoral: Universidad de Barcelona, Cataluña). Recuperado de https://www.tdx.cat/handle/10803/2658#page=2 [2020, 01 de junio].

Pagnone, L. (2015). Materia Auditoría interna y operativa. Maestría en Auditoría. *FACEA*. *Universidad Católica de Córdoba*, Argentina.

Perfumo, S. (2013). *Entorno informático del ente auditado. Su impacto en la evaluación del riesgo de auditoría* (Tesis de maestría. Universidad Católica de Córdoba, Argentina).

Pinzón, M. F. G., y Sanabria, J. S. G. (2013). Aplicación del estándar ISO/IEC 25012 en el modelo de datos conceptual entidad-relación. *Revista Facultad de Ingeniería, 22* (35), 113-125. Recuperado de https://www.redalyc.org/pdf/4139/413940774009.pdf [2020, 29 de junio].

Pungitore, J. L. (2013). *Sistemas Administrativos y Control Interno* (2da ed.). Buenos Aires: Osmar D. Buyatti.

Red Global de Conocimientos en Auditoría y Control Interno (2013). Política para la administración de claves. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2013). Política para la administración y uso del software. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2013). Política para realizar copias de seguridad. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2016). Buenas prácticas para gestionar las copias de seguridad. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2016). Buenas prácticas para gestionar los activos de TI. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2016). Política para la clasificación y administración de datos. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2016). Política para la seguridad de la información. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2017). Buenas prácticas para gestionar los riesgos en la información. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2017). Buenas prácticas para prevenir el fraude electrónico. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2017). Carta de recomendaciones del proceso de controles generales de tecnología. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2017). Factores de riesgos en la tecnología para las empresas. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2017). Política para el uso del correo electrónico. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2018). Autoevaluación del sistema de control interno de un proceso de controles generales de TI. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2018). Buenas prácticas en ciberseguridad. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2018). Checklist para preguntas sobre riesgo cibernético para el Consejo de Administración. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2018). Cuestionario controles de acceso a sistemas de información. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2018). Guía para el control de autorización. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2018). Guía para la evaluación de aplicaciones. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2018). Política de respuesta a incidentes. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2018). Riesgos inherentes de un proceso de controles generales de tecnología ITGC. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2019). Buenas prácticas de auditoría interna para identificar los nuevos riesgos en las organizaciones. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2019). Controles de un proceso de tecnología ITGC's. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2019). Diagnóstico factores de riesgo para la integridad de la información. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2019). Política para la administración de la información TI. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2019). Política para la gestión de cambios de TI. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2020). Buenas prácticas para gestionar los riesgos cibernéticos desde COSO ERM. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2020). Matriz para evaluar controles generales de tecnología ITGC. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Red Global de Conocimientos en Auditoría y Control Interno (2020). Política para la asignación de niveles de autorización. Recuperado de https://www.auditool.org/ [2020, 22 de julio].

Rehage K., Hunt S. y Nikitin F., (2008). Global Technology Audit Guide (GTAG) 11. Developing the IT Audit Plan. Recuperado de https://www.iiacolombia.com/resource/guias/GTAG11.pdf [2020, 23 de agosto].

Richards D. A., Oliphant A. S. y Le Grand C. H. (2005). Global Technology Audit Guide (GTAG) 1. Information technology controls. Recuperado de https://www.iiacolombia.com/resource/guias/GTAG1.pdf [2020, 23 de agosto].

Rodríguez de Ramírez, M. D. C. (2004). La contabilidad y el impacto de las tecnologías de la información y las comunicaciones. *Contabilidad y Auditoría,* 19, Año 10. Recuperado de http://www.economicas.uba.ar/wp-content/uploads/2016/03/La_contabilidad_y_el_impacto_de_las_tecnologias_de_la_informacion_y_las_comunicaciones.pdf [2020, 22 de noviembre].

Rusenas, R. O. (2011). Control interno (1era ed.). Buenos Aires: La Ley.

Sal Paz, J. C. (2010). Notas sobre las Tecnologías de la Información y de la Comunicación. *Sociedad y Discurso*, 17, 44-72. Recuperado de https://ri.conicet.gov.ar/bitstream/handle/11336/75432/CONICET_Digital_Nro.06bddbc9-9e56-4c50-b619-cc0ed2859813_A.pdf?sequence=2&isAllowed=y [2020, 18 de abril].

Schoderbek, C. G., Schoderbek, P. P., y Kefalas, A. G. (1984). El enfoque de sistemas en C. G. Schoderbek, P. P. Schoderbek y A. G., Kefalas. *Sistemas administrativos* (3era ed) (p. 5-34). Buenos Aires: El Ateneo.

Serrano González, S., y Zapata Lluch, M. (2003). Auditoría de la información, punto de partida de la gestión del conocimiento. *El profesional de la información*, *12* (4), 290-297. Recuperado de http://www.elprofesionaldelainformacion.com/contenidos/2003/julio/5.pdf [2019, 29 de noviembre].

Sinay, S. (2017). *Intoxicados: cómo la información excesiva arruina nuestras vidas.* (1era ed.). Buenos Aires: Paidós.

Soy i Aumatell, C. (2003). La auditoría de la información, componente clave de la gestión estratégica de la información. *El profesional de la información, 12* (4), 261-268. Recuperado de http://www.elprofesionaldelainformacion.com/contenidos/2003/julio/2.pdf [2020, 29 de julio].

The Institute of Internal Auditors (2007). GAIT Methodology. A risk-based approach to assessing the scope of IT general controls. Recuperado de https://www.iiacolombia.com/resource/guias/GAIT_Methodology.pdf [2020, 23 de agosto].

Urteaga, E. (2010). La teoría de sistemas de Niklas Luhmann. *Contrastes: revista internacional de filosofía*, (15), 301-317. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=3283017 [2020, 08 de abril].

Volpentesta, J. (2004). *Sistemas administrativos y sistemas de información* (1ª ed.). Buenos Aires: Osmar D. Buyatti.

Von Bertalanffy, L. (1976). *Teoría general de los sistemas* (1era ed.). México: Fondo de Cultura Económico.

Wiener, N. (1948). *Cybernetics or control and communication in the animal and the machine.* (2da ed.). USA: The MIT Press.

Wiener, N. (1969). *Cibernética y sociedad* (2da ed.). Buenos Aires: Sudamericana.

8. Anexo: entrevista

1) *¿Suelen tener las organizaciones un conocimiento profundo sobre los problemas que presentan sus sistemas de información mediados por tecnología? Si tuvieras que establecer un orden sobre dicho conocimiento, ¿dirías que se observa en mayor medida en los mandos altos, medios o bajos? ¿Cuáles son tus motivos para dicho orden?*

2) *Considerando las labores de auditoria realizadas, ¿En qué medida las observaciones a los procedimientos o controles tienen como origen problemas relacionados con la tecnología o con los contextos informatizados?*

3) *Si tuvieras que enumerar, a rasgos generales, cuales son los problemas o factores de riesgos más comunes que presentan los sistemas de información mediados por tecnología, ¿Cuál sería tu ranking y por qué?*

4) *Según tu experiencia y teniendo en cuenta aquellas organizaciones que aplican gestión de riesgos con las que has trabajado ¿Incluyen dentro de dicha gestión al riesgo tecnológico?*

5) *¿Cuál consideras que es la percepción que las organizaciones poseen frente a los riesgos relacionados con la tecnología? ¿A qué atribuís dicha percepción?*

6) *A rasgos generales y teniendo en cuenta los atributos y características de la información (integridad, confidencialidad, relevancia, comparabilidad, claridad o comprensibilidad, oportunidad, verificabilidad, accesibilidad o disponibilidad, precisión, libertad de error, entre otras), ¿Cuáles crees que son los que más suelen verse afectados frente a los contextos tecnológicos? ¿A qué asocias dicha frecuencia? ¿Cuáles de esos atributos o características suelen verse más afectados de forma negativa y cuáles de forma positiva? ¿Cuáles consideras que son los motivos?*

7) *Según tu experiencia, ¿Cuál o cuáles consideras que son los aspectos críticos a tener en cuenta al auditar el proceso de generación de información de una organización en contextos informáticos?*

8) *Si tuvieras que pensar en cómo ha afectado el contexto tecnológico a las evidencias de auditoría, ¿Cuáles dirías que son las consecuencias más importantes? ¿Consideras que son positivas o negativas?*

9) *Si tuvieras que considerar la importancia del escepticismo profesional frente a las auditorías de sistemas de información mediados por la tecnología ¿Qué tan importante es y cuáles son tus motivos?*

10) *Según tu experiencia y en base a las labores de auditoría realizadas, ¿Qué tan frecuentemente incluís dentro de tu equipo de trabajo a expertos en informática (ingenieros o analistas)? ¿Qué consideraciones tomas en cuenta a la hora de incluirlos o excluirlos?*