UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE CIENCIAS ECONÓMICAS

DOCTORADO

TESIS

PROPUESTA DE UN MODELO CONTABLE QUE REFLEJE EL CARÁCTER DE ACTIVO QUE LA INFORMACIÓN CORPORATIVA REPRESENTA PARA UNA ENTIDAD BANCARIA

Alumno: Diego Sebastián Escobar

Directora de Tesis: Elsa Beatriz Suarez Kimura

Miembros del Tribunal de Tesis:

Graciela María Scavone

Carmen Stella Verón

Walter Rene Chiquiar

Fecha de defensa de la Tesis: 22-8-22

- Resumen

En la actualidad, el uso masivo de las tecnologías de la información y comunicación como medios para generar, almacenar, transferir y procesar información, se ha convertido en un elemento indispensable en gran parte de las organizaciones para el desarrollo de sus actividades.

En este contexto, la información corporativa comenzó a depender progresivamente de la infraestructura tecnológica, surgiendo nuevos métodos en el almacenamiento, procesamiento, control y resguardo.

Sobre esta problemática, las entidades bancarias comenzaron a implementar procedimientos administrativos para identificar, registrar e inventariar la información bajo su custodia, responsabilidad y resguardo.

En el marco de la presente investigación se plantea abordar la contextualización de un Modelo Contable que contemple a los activos de información existentes en las

entidades bancarias, contrastando con los elementos de la Teoría General Contable propuesta por los autores: Carlos Luis García Casella, Luisa Fronti de García y María del Carmen Rodríguez de Ramírez.

Si bien hay antecedentes del pronunciamiento de distintas disciplinas sobre aspectos legales, normativos y tecnológicos acerca del resguardo de la información, no se la ha definido o analizado desde el marco teórico de la contabilidad. Basándose en eso, se propone identificar los elementos de un Modelo Contable para el tratamiento de la información como un activo.

- Palabras Clave: CONTABILIDAD – NO MONETARIA - INFORMACIÓN

- Tabla de contenido

- Prólogo

La presente tesis doctoral en Ciencias Económicas es el resultado de numerosas horas de investigación, intentando reflejar en el mismo un aporte en la disciplina contable y en la profesión de Contador Público en la República Argentina.

En primer lugar, el autor desea dedicar este logro a Elsa Beatriz Suarez Kimura por contagiar todo el entusiasmo ya que sin su ayuda esta obra no hubiera sido posible.

En segundo a su familia, Claudia Teresa Pszytula, Valentino Emanuel Pelella, Julieta Carolina Escobar, Jorge Horacio Escobar, Beatriz del Valle Salvador, Alérico Tomás Escobar, Alejandra Bak y Francisco Pszytula.

A quienes le han abierto puertas dando oportunidades en diferentes ámbitos: Luisa Fronti de García, Carlos Luis García Casella y Elizabeth Ierino. Y por último a esas personas que han tenido paciencia a lo largo de este tiempo: Ariel Cister, Laura Acevedo, Sebastián Ariel Ruau, Juan Manuel Ostera, Verónica Gabriela Cacciabue y Marisa Andrea Valcárcel.

Diego Sebastián Escobar

- Nómina de abreviaturas

AAIP: Agencia de Acceso a la Información Pública

AFIP: Administración Federal de Ingresos Públicos.

AIC: Asociación Interamericana de Contabilidad.

ANPCyT: Agencia Nacional de Promoción Científica y Tecnológica.

CABA: Ciudad Autónoma de Buenos Aires.

CMDB: Configuration Management Database.

COBIT: Objetivos de Control para Información y Tecnologías Relacionadas.

CODECE: Consejo de Decanos de Ciencias Económicas.

COSO: The Committee of Sponsoring Organizations of the Treadway Commission.

CPCECABA: Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires.

DLP: Data Loss Prevention.

exDNPDP: ex Dirección Nacional de Protección de Datos Personales.

FACPCE: Federación Argentina de Consejos Profesionales en Ciencias Económicas.

FONCyT: Fondo para la Investigación Científica y Tecnológica

IASB: International Accounting Standards Board.

IEC: International Electrotechnical Commission.

IFAC: International Federation of Accountants.

IGJ: Inspección General de Justicia.

IRAM: Instituto Argentino de Normalización y Certificación.

ISO: International Organization for Standardization.

NIST: National Institute of Standards and Technology

PCI-DSS: Payment Card Industry Data Security Standard.

RT: Resolución Técnica aprobada por la FACPCE.

RT: Resolución Técnica.

SGSI: Sistema de Gestión de Seguridad de la Información.

SIEM: Security Information and Event Management.

TGC: Teoría General Contable

Cuerpo Introductorio

Introducción

A. Justificación

La Real Academia Española (RAE) define a la información como un "*grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente*" (2020). En el caso de las entidades bancarias, debido al uso de los canales electrónicos, se gestionan importantes volúmenes de datos transaccionales convirtiéndose en uno de los elementos mas importantes en los procesos de negocio.

Considerando la defínción de Patrimonio dispuesta por el Dr. Osvaldo Chaves en el desarrollo de la Teoría General Contable, la define *"como el conjunto de bienes, derechos y obligaciones pertenecientes al ente. Cabe agregar que al hablar de bienes y derechos (en principio, activo, en el lenguaje contable) y de obligaciones (pasivo)."* (Chaves, Chyrikins, Dealecsandris, Pahlen Acuña, & Viegas, 1998). Asimismo, plantea que:

> *"los recursos pueden clasificarse según su grado de permanencia en el patrimonio del ente; es posible diferenciar aquellos de rápida movilidad de*

otros de carácter permanente. Para proceder a su distinción se debe considerar en los bienes su mayor o menor grado de convertibilidad en dinero. Otra distinción radica en que los primeros le permiten al ante el desarrollo de su actividad específica, mientras que los indicados en segundo término le brindan al ente una estructura permanente para facilitar las mencionadas actividades."

Desde esa contextualización de la TGC, se puede clasificar a la información existente en las organizaciones. Pero en el caso particular de la información, no toda posee un valor de cambio cuantificable monetariamente, lo que requiere un análisis particular para poder describirla, identificarla, medirla y registrarla, dentro de los parámetros establecidos en la disciplina contable.

En la posición del autor de la presente tesis es posible identificar que la información cumple con las características del mismo, formando parte del patrimonio de las entidades, dependiendo inevitablemente del soporte de la misma. Los datos en custodia de las entidades constituyen un activo que debería ser identificado, inventariado, administrado y controlado en todas sus formas, ya sea, en datos e información existentes en soporte de papel, en conocimiento de los empleados, o bien resguardados o delegados en terceras partes.

Sobre esta problemática las entidades bancarias, comenzaron a implementar procedimientos administrativos para identificar, registrar y resguardar la información bajo su custodia, requiriéndose nuevos métodos en el almacenamiento, procesamiento, control y resguardo de este activo. En esta línea, el Banco Central de la República Argentina (BCRA), organismo regulador para las

entidades bancarias, en sus Comunicaciones “A” 4609, 5374, 6017 y 6354 estableció requisitos mínimos en relación con la administración de la información, los sistemas y canales electrónicos.

La información como parte del patrimonio existente en los entes, ha sido considerada como un activo intangible autogenerado o más precisamente como parte del capital intelectual formando parte de la llave de negocio o plusvalía de los entes. En relación con su reconocimiento en el segmento contable financiero, el autor Enrique Fowler Newton (Cuestiones Contables Fundamentales, 2020) establece que:

> *“En lugar de utilizar una definición de "intangible" coherente con el lenguaje común, el IASB la restringió a los intangibles identificables, dejando fuera del concepto de intangible a los que solamente pueden venderse junto con una entidad o un negocio, como una plusvalía (llave de negocio) o los costos de puesta en marcha de un negocio. Lo razonable habría sido definir intangible de una manera más amplia, (…) y definir el tratamiento contable de los restantes activos intangibles no identificables.”*

El autor Mario Biondi en su artículo (Los Bienes intangibles y los intereses en los costos de producción analizados con enfoque en la contabilidad de gestión, 2012) indica que:

> *“Podríamos mencionar como intangibles, susceptibles de mostrarse en los estados financieros, entre otros, los siguientes, identificados como: Patentes de invención, Marcas de fábrica, Plusvalía mercantil (comúnmente “Llave de Negocio”), gestión de terceros, Gestión del personal.*

La “gestión del personal” se conoce habitualmente como “capital intelectual”. Verdaderamente comprende no sólo la gestión pensante sino también la gestión física sin la cual muchas cosas no podrían concretarse.”

Asimismo, la autora Ugalde Binda en su artículo (Capital intelectual del emprendedor y la innovación, 2019) establece que “*es clara la forma en que los elementos del capital intelectual interactúan para propiciar la mejora continua: las ideas se gestan en el capital humano, pero se requiere de una infraestructura apropiada, compromiso con la calidad y buena organización para seleccionar las ideas más convenientes, y afinarlas hasta que sean factibles de implementación*”. Este planteo concuerda con los autores Vázquez y Bongianino de Salgado (Los activos intangibles y la contabilidad, 2002, pág. 15) que la consideran un activo intangible parte del capital intelectual pero todavía no se ha planteado doctrinariamente una definición acorde a las necesidades actuales.

En los últimos años, en la disciplina contable se pueden identificar múltiples líneas de investigación abocadas a los diferentes segmentos. Puede destacarse que ya desde fines de la década de los sesenta Richard Mattessich identificó a la Contabilidad en dos líneas bien definidas, las que se dedican a la contabilidad monetaria y las que se refieren a la contabilidad no monetaria (Accounting and analytical methods. Measurement and projection of income and wealth in the micro- and macro-economy., 1964).

En este contexto, se pretende encarar el abordaje de los activos de información corporativa desde la perspectiva contable no monetaria, y en base a los elementos de la Teoría General Contable propuestos por Carlos Luis García Casella Luisa

Fronti de García y María del Carmen Rodríguez de Ramírez (2001), identificar los pertinentes para contextualizar un Modelo Contable propio para los activos de información existentes en las entidades bancarias.

B. Identificación del aporte

Los activos de información están presentes en todas las organizaciones, pero en las entidades bancarias reguladas por el BCRA, es posible identificar procesos de registración de este tipo de activo de forma sistemática y organizada.

Dada la forma en que se manifiesta la identificación de este tipo de activo, es posible estructurarla en un Modelo Contable con características propias dedicado a la información en las entidades bancarias.

El resultado de la presente investigación se verá reflejado en la identificación de los elementos pertinentes de la Teoría General Contable que permitan plantear las bases de un Modelo Contable Microsocial (perteneciente al segmento de contabilidad de gestión no monetaria).

C. Planteo del problema

Se establecen los siguientes interrogantes para la investigación:

- ¿Cómo se realiza el reconocimiento patrimonial de los activos de información?

- ¿Cómo se define a los activos de información actualmente en las diferentes disciplinas?
- ¿Pueden identificarse diferentes modelos de medición, clasificación y exposición de la información?
- ¿En qué segmento contable podrían incluirse los activos de información de una entidad bancaria?
- ¿Qué sujetos participantes, normas y mejores prácticas se pueden identificar para el tratamiento de esta clase de activo?
- ¿Cuáles serían los elementos de la Teoría General Contable de los activos de información en el Modelo Contable propuesto como resultado de esta investigación?

D. Objetivos

En el marco de la presente investigación se establecen los siguientes objetivos:

Objetivo general

Identificar los elementos básicos del dominio del discurso contable de la Teoría General para contextualizar un Modelo Contable aplicado al reconocimiento de los activos de información existentes en las entidades financieras.

Objetivos específicos

a. Definir doctrinariamente a los activos de información, clasificarlos e identificarlos.

b. Identificar los elementos de la Teoría General Contable propuesta por Carlos Luis García Casella, Luisa Fronti de García y María del Carmen Rodríguez de Ramírez para la contextualización de un Modelo Contable para los activos de información.

c. Describir el marco teórico de la contabilización de los activos de información en las Entidades Financieras.

d. Identificar modelos de medición específicos para los activos de información.

e. Plantear teóricamente a qué segmento contable pertenece este tipo de contabilidad e identificar los entes participantes.

f. Identificar el marco normativo para esta clase de activos previsto por la Inspección General de Justicia (IGJ), el Banco Central de la República Argentina (BCRA) y la Agencia de Acceso a la Información Pública (AAIP).

g. Identificar contrastaciones empíricas sobre mejores prácticas existentes en el mercado para el análisis, gestión y control de este tipo de activos existentes en las entidades bancarias, en servicios delegados en terceros o en conocimiento del personal.

h. Proponer el dominio o universo del discurso contable en la que encuadrarían los activos de información.

E. Descripción sobre el uso de los elementos para una Teoría General Contable

En el desarrollo de la presente investigación y con el objetivo de contrastar los elementos que deben tener los Modelos Contables, se tomará como base el proyecto de investigación dirigido por el Dr. Carlos Luis García Casella y codirigida por las doctoras: Luisa Fronti de García y María del Carmen Rodríguez de Ramírez denominado "Elementos para una Teoría General de la Contabilidad" en la Universidad de Buenos Aires.

En el mismo, los autores plantean ocho problemas que deben ser considerados:

"1 DOMINIO O UNIVERSO DEL DISCURSO CONTABLE

2 NATURALEZA O STATUS EPISTEMOLÓGICO DE LA CONTABILIDAD

3 RELACIONES DE LA CONTABILIDAD CON OTRAS DISCIPLINAS

4 SEGMENTACIÓN O UNIDAD CONTABLE ABSOLUTA

5 SISTEMAS CONTABLES

6 MEDICIÓN

7 PERSONAS O SUJETOS DE LA ACTIVIDAD CONTABLE

8 MODELOS EN LA TEORÍA GENERAL CONTABLE" (García Casella, Fronti de García, & Rodríguez de Ramírez, 2001)

En el desarrollo de las conclusiones del citado proyecto, se editó un libro con la misma denominación bajo la coordinación del Dr. García Casella, que es utilizado

como material de lectura obligatoria en las cátedras de Teoría Contable de la Facultad de Ciencias Económica en la Universidad de Buenos Aires.

Como se indicó precedentemente, para poder contrastar los elementos necesarios para definir un Modelo Contable Alternativo para el tratamiento de la información en entidades financieras, se contrastarán considerando los planteos de los problemas y las Leyes Teóricas propuestas para el desarrollo de la Teoría General Contable aplicable a todos los segmentos existentes.

F. Hipótesis

Las hipótesis planteadas en la presente investigación son las siguientes:

H1: La contabilización de los activos de información existentes en las entidades bancarias conforma un sistema contable con características propias del segmento no monetario.

H2: La contabilización de los activos de información se relaciona con otras disciplinas como la Tecnología y la Seguridad de la información, sin dependencia de ellas.

H3: En las entidades bancarias se puede identificar un sistema de información dedicado la recolección y registro de eventos de seguridad y control para los activos de información.

H4: La contabilización de activos de información se ocupa de mediciones cualitativas y cuantitativas no monetarias para poder emitir informes para la toma de decisiones.

H5: En la contabilización de activos de información participan personas o sujetos abocadas a la tarea.

H6: El universo del discurso contable identificado en el tratamiento de la información en las entidades bancarias, tiene características propias no monetarias, en la identificación, medición, valorización y exposición.

En base a los elementos descriptos por los autores Carlos Luis García Casella, Luisa Fronti de García y María del Carmen Rodríguez de Ramírez en el dominio del discurso contable, se deberían identificar los siguientes elementos:

1- Informes sobre los activos de información de uso externo a los emisores.

2- Personas, grupos de personas y áreas emisoras de los diversos informes contables sobre activos de información.

3- Personas revisoras, auditores o áreas de auditoría que opinan sobre la calidad de los informes contables sobre los activos de información.

4- Personas, grupos de personas usuarias o sectores destinatarias de los diversos informes contables de activos de información.

5- Personas, grupos de personas o entes reguladores de los distintos informes contables de activos de información.

6- Microsistemas contables de activos de información propios de cada ente.

7- Macrosistemas contables de activos de información definidos en la Ciudad Autónoma de Buenos Aires.

8- Modelos contables de activos de información necesarios para determinar variables relevantes en diversas situaciones.

9- Informes contables de uso interno en cada ente.

10- Informes de activos de información contables de organismos gubernamentales.

11- Informes de activos de información contables macroeconómicos.

12- Informes de activos de información contables macrosociales.

13- Informes de activos de información contables microsociales.

14- Segmento contable de activos de información.

H7: La contabilización de activos de información en las entidades bancarias cumple con los requisitos para ser considerado un modelo contable alternativo del segmento no monetario.

F. Alcance de la investigación

En el contexto de la investigación se establecen los siguientes alcances:

Se analizarán los activos de información presentes en las entidades bancarias reguladas por el BCRA dado que en investigaciones preliminares desarrolladas por el doctorando se identificó que el sector en donde está presente la contabilización de la información en forma obligatoria es en este tipo de entidades.

No se analizará ni planteará la medición monetaria de los activos de información.

El cuerpo principal se articulará de la siguiente manera:

- Capítulo I: Activo de información: Definición, características e identificación.
- Capítulo II: Identificación de los elementos para la descripción de un Marco conceptual para el tratamiento contable no monetario de los activos de información.
- Capítulo III: Dominio del discurso contable de los activos de información.
- Capítulo IV: Naturaleza epistemológica de la contabilización de activos de información.
- Capítulo V: Vinculación de la contabilización de los activos de información y otras disciplinas.
- Capítulo VI: Segmentación de la contabilización de los activos de información.
- Capítulo VII: Identificación del sistema contable de activos de información.
- Capítulo VIII: Modelos teóricos para la medición de los activos de información.
- Capítulo IX: Personas y sujetos en la actividad contable de los activos de información.
- Capítulo X: Informes contables no monetarios de activos de información en Entidades Bancarias.
- Capítulo XI: Identificación de Normas Contables Legales para el sistema de activos de información.

- Capítulo XII: Identificación de normas y estándares para el control de los activos de información.
- Capítulo XIII: Conclusiones.

G. Metodología de la investigación

Para responder a los objetivos de investigación propuestos, en la presente tesis se realizará un estudio descriptivo basándose en el reconocimiento y articulación de los conceptos y variables identificadas en la contabilización de los activos de información. Para poder describir el fenómeno, se realizará un estudio de casos en donde se analizarán entidades bancarias en el ámbito de la Ciudad Autónoma de Buenos Aires.

Asimismo, se llevarán a cabo relevamientos bibliográficos que permitan actualizar los antecedentes correspondientes a las propuestas emitidas por diversos organismos internacionales como la Asociación Interamericana de Contabilidad (AIC) y la International Federation of Accountants (IFAC), como también nacionales como el Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires (CPCECABA), Consejo de Decanos de Ciencias Económicas (CODECE), IGJ, BCRA y AAIP en relación con el resguardo, gestión y control de la información; y se efectuará un análisis conceptual de las teorías que subyacen, así como las posibilidades de integración de las mismas. El monitoreo de nuevos pronunciamientos será una constante que posibilitará asegurar la validez de las conclusiones parciales y finales.

Cuerpo Principal

Capítulo I

1. Activo de información: Definición, características e identificación

1.1. Introducción

El concepto de activo contable se ha analizado numerosas veces desde la perspectiva del segmento patrimonial, en donde fue enunciado en el Marco Conceptual del International Accounting Standards Board (IASB) como *"un recurso económico presente controlado por la entidad como resultado de sucesos pasados".* Si bien esta definición es considerada en el segmento contable financiero, en el presente capítulo se plantea identificar una definición de activo de

información que cumpla con las características para un Modelo Contable no monetario para entidades bancarias.

1.2. Conceptualización de activo contable

La Real Academia Española (2020) define al dato como "*Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho*" y a la información como un "*grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente*" (Celeita, 2020). Con estas definiciones se puede identificar que los procesos de negocio se basan en este tipo de elemento constantemente, y los mismos pueden ser almacenados en múltiples soportes y encontrarse en custodia o no de las entidades.

En el ámbito mundial, se ha relacionado a la contabilidad y a la información desde la temática de la tecnología y la seguridad desde la perspectiva del procesamiento de datos, por ejemplo, el autor Qayssar y equipo manifiestan que *"El sector bancario generalmente necesita una mejora de la tecnología y está más inclinado a optar por subcontratar ante tales circunstancias.* (2022)*."* [i]

En esa misma corriente, se puede identificar en las publicaciones del American Accounting Association en donde esta relación se manifiesta en el rol del auditor o revisor: *"encontramos que la calidad de la relación entre la auditoría interna y las funciones de seguridad de la información se asocia positivamente con las percepciones sobre el valor proporcionado por la auditoría interna y, lo que es más*

importante, con las medidas de eficacia general de los esfuerzos de seguridad de la información de la organización"[ii] (Steinbart, Raschke, Gal, & Dilla, 2021). Como, por ejemplo, indican que "el *empleo de mecanismos de tecnología de la información en el AIS contribuyó a reducir los errores no intencionales y al desarrollo de la profesión de auditoría*"[iii] (Jasim & Raewf, 2022). O en la aplicación de diversos tipos de monitoreos, como de "*seguridad y control general para las organizaciones; seguridad y control general para Tecnologías de la Información (TI), y controles de aplicación para el procesamiento de transacciones.*"[iv] (Bawaneh, 2022)

En las investigaciones en donde se relaciona la contabilidad y la ciberseguridad, son mayoritariamente en el análisis de un tipo de incidente, o desastre operativo y dada la dependencia de los datos se reconoce que "*la importancia de la seguridad de la información y el trabajo contable está en crecimiento (…) la falta de un buen análisis del sistema de información contable dará lugar a la divulgación de información financiera, e incluso perjudicará los intereses económicos de las empresas en casos graves*" (Wang, 2021) y además "*cada vez aparecen más artículos en estas publicaciones que analizan los métodos de seguridad para las nuevas tecnologías*."[v] (Henry, 2020)

En este sentido estamos en el proceso de un cambio cultural en donde la información y la dependencia a la infraestructura tecnológica cumple un rol ineludible en las organizaciones, como manifiestan los autores Petratos y Faccia: "*existe un riesgo cada vez mayor de seguridad cibernética para los sistemas de información contables, que puede considerarse parte de la infraestructura crítica, en ese sentido, la evaluación de los riesgos de seguridad cibernética es esencial.*"[vi]

(2019) y por lo tanto conocer sus riesgos y sus amenazas, se necesita que "las *organizaciones trabajen para superar la reticencia de los empleados al cambio para mejorar el cumplimiento de la política de seguridad*"[vii] (Malimage, Raddatz, Trinkle, & Crossler, 2020); si bien estas concepciones son fundadas desde el rol de contador o auditor, no se planteó la necesidad de un modelo contable alternativo para la registración de la información.

Con el objetivo de conceptualizar la definición de información como activo, resulta indispensable partir de la definición de Patrimonio desde la perspectiva de la Teoría General Contable. Si bien, la siguiente definición puede aplicarse al segmento contable patrimonial o financiero, no resulta excluyente para aplicarlos en otros segmentos monetarios o no monetarios.

En el libro Teoría Contable, el autor Osvaldo Chaves define al Patrimonio *"como el conjunto de bienes, derechos y obligaciones pertenecientes al ente. Cabe agregar que al hablar de bienes y derechos (en principio, activo, en el lenguaje contable) y de obligaciones (pasivo)."* (Chaves, Chyrikins, Dealecsandris, Pahlen Acuña, & Viegas, 1998). En la misma línea, plantea que en la organizaciones existen recursos, y los mismos pueden *"clasificarse según su grado de permanencia en el patrimonio del ente; es posible diferenciar aquellos de rápida movilidad de otros de carácter permanente."*

Desde esta primera interpretación y desde esa contextualización de la TGC, se puede clasificar a la información como un recurso existente en las organizaciones, con un grado de permanencia en el patrimonio.

Asimismo, el Dr. Chaves manifiesta que *"para proceder a su distinción se debe considerar en los bienes su mayor o menor grado de convertibilidad en dinero",* y relación a su movilidad, algunos *"le permiten al ente el desarrollo de su actividad específica o le brindan al ente una estructura permanente para facilitar las mencionadas actividades."*

Siguiendo con esta interpretación, en el caso particular de la información no toda posee un valor de cambio cuantificable monetariamente, dado que por las características físicas se relaciona con el soporte en donde la misma es almacenada. Desde este concepto, se puede definir como una *"*estructura*"* permanente para facilitar las tareas de los entes.

Asimismo, la información como parte del patrimonio existente en los entes ha sido considerada por varios autores como un activo intangible parte del capital intelectual o de la plusvalía (llave de negocio); pero en el marco de la presente investigación se requiere un análisis particular para poder describirla, identificarla, medirla y registrarla, dentro de los parámetros establecidos en la disciplina contable.

Tomando como base las definiciones precedentes, la información y los datos procesados en las entidades bancarias, se encuentran bajo su custodia y consecuentemente forman parte de los recursos disponibles que poseen. Se recuerda que en la presente investigación se analizará desde la perspectiva de la contabilidad no monetaria, ya que la contabilización en el segmento financiero de los activos intangibles no se encuentra en el alcance de la presente tesis.

1.3. Definición de activo de información

La terminología “activo de información” ha sido definida en la serie IRAM/ISO/IEC 27.000 como a “los datos o conocimientos que tienen valor para una organización”. Si bien la definición es lo correctamente amplia, es complejo identificar y sistematizar a la información existente en las entidades bancarias, para ello se analizará la aplicación de la teoría de la propiedad y la de la entidad de la disciplina contable.

Las autoras Rodríguez de Ramírez y Marcolini destacan que, desde la concepción doctrinaria, “*la determinación de la existencia de un sujeto contable es fundamental para su caracterización como entidad informativa*” (2013).

En el caso de la contabilización de los activos de información existente en las entidades bancarias se encuentra bajo su custodia, e independiente de su origen[viii] se encuentra controlada por ellos mismos y asimismo forma parte de la estructura de los entes para poder desarrollar sus actividades.

Con el objetivo de analizar este concepto, se analizará desde la visión de la Teoría de la Entidad y la Teoría de los propietarios. Según el autor Moonitz (1951) *“La teoría de la entidad parte de la existencia de una entidad económica o de negocios, compuesta por unidades jurídicamente independientes en las que una ejerce el control común, originado en la propiedad compartida de la entidad.”*

Como indican las autoras, *“Moonitz concibe a la entidad contable (grupo), emisora de los estados contables consolidados, como una unidad de negocios cuyos proveedores de capital son dos clases de accionistas: los mayoritarios y los*

independientes. Las relaciones entre las empresas que conforman el grupo pueden ser de subordinación y de cooperación." (Ramírez & Marcolini, 2013)

Si bien, el autor aplicaba esta teoría a la consolidación de los Estados Financieros, las entidades financieras controlan y mantienen bajo su custodia información que pertenecen a terceros involucrados, como los de clientes, empleados y proveedores. La aplicación de esta Teoría en el caso particular de la contabilización de activos de información es la existencia de un conjunto de datos que cuya propiedad no es exclusiva de la entidad, sino, que corresponden a otras personas humanas y jurídicas, y en el caso de las entidades financieras, estas ejercen el control real de la información. Por lo tanto, la información existente en las entidades corresponde a dos tipos de titulares, los que son titulares y los que poseen la custodia de los datos.

En el contexto de la contabilización de los activos de información se identifica que el objetivo de esta Teoría es el proporcionar datos o información útil a quienes controlan los activos de información, sin dejar de brindarle garantías a los titulares de los mismos.

Al analizar la Teoría del propietario, en la cual se indica que "*para la preparación de información consolidada concibe al ente contable (grupo) como una extensión de la propiedad que detenta la sociedad poseedora de la mayoría de capital de las sociedades que integran el grupo"* (Ramírez & Marcolini, 2013).

Este enfoque aplicado a los activos de información, se pueden sintetizar que existe un interés en las entidades que posee la custodia de la información por sobre la

titularidad de otras personas físicas y jurídicas. En este planteo, los particulares de los datos serían ajenos a la información ya que los datos solamente corresponderían a la entidad que tiene su custodia.

Bajo estas definiciones, para un reconocimiento eficiente de los datos e información, es mejor considerar como activo de información a todo elemento que contenga, almacene, procese o transmita información de la entidad. Con esta última definición, se pueden identificar dos clases de activos de información: los que se encuentran en custodia de la organización y los que se encuentran en custodia de terceros. A continuación, se desarrollarán las principales categorías de activos de información existentes en las entidades bancarias.

1.4. Categorías de activo de información

Considerando activo de información a todo elemento que contenga, almacene, procese o transmita información de la entidad, se identifican los siguientes elementos teniendo en cuenta sobre a quién recae la custodia de los datos:

1.4.1. Información en custodia de la organización

Al identificar la información es custodia de las entidades, se pueden destacar:

- **N1 – Procesos:** Corresponde a los macroprocesos, procesos y procedimientos que existen en las entidades.

- **N2 – Documentación en papel:** Corresponde a toda la información existente en formato impreso.
- **N3 – Repositorios de archivos y bases de datos:** Corresponde a todos los archivos de información, repositorios y bases de datos instaladas.
- **N4 – Plataforma de Software:** Corresponde a todos las aplicaciones y sistemas operativos instalados en la entidad.
- **N5 – Plataforma de Hardware:** Comprende a toda la infraestructura de Hardware y Telecomunicaciones existente [ix] . Ejemplos: Servidores, computadoras de escritorio, computadoras portátiles, teléfonos inteligentes, discos de almacenamiento, etc.
- **N6 – Sitios físicos:** Corresponde a todos los sitios en donde se desarrollan las actividades de la entidad.

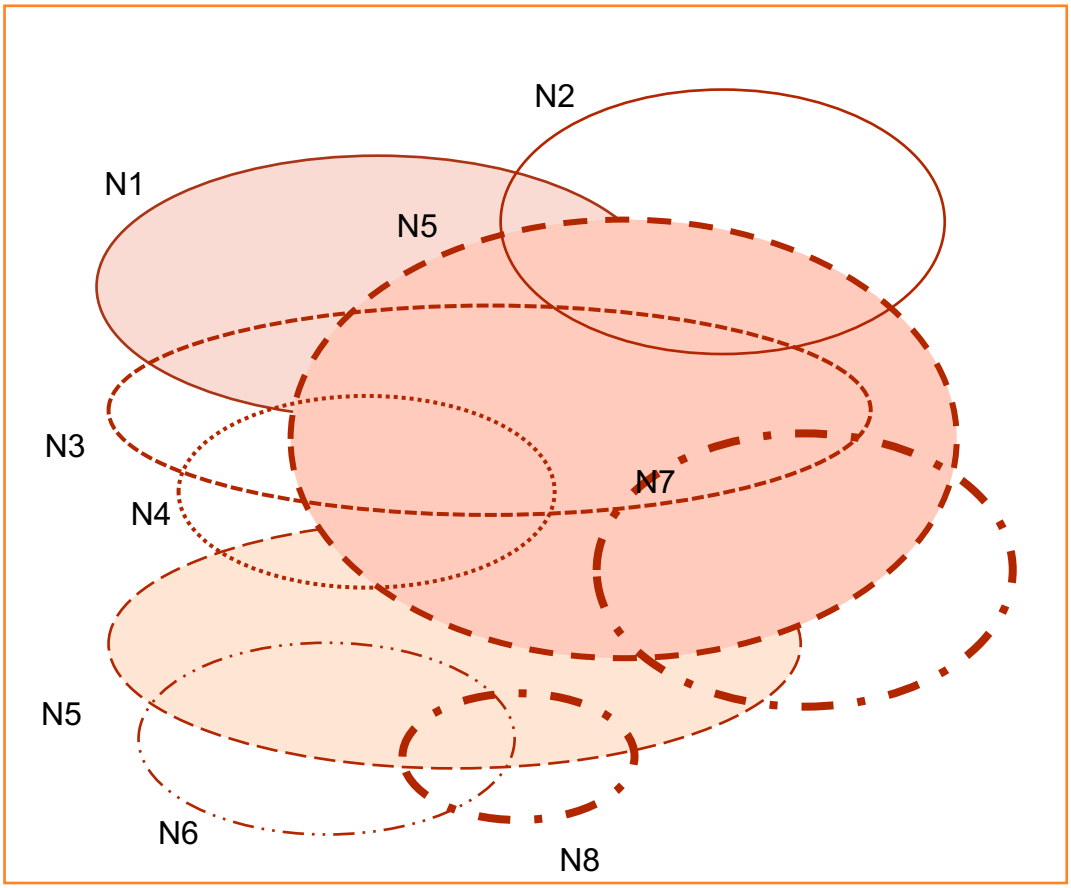
1.4.2. Información en custodia de terceras partes:

Al identificar la información es custodia de terceras partes, se pueden destacar:

- **N7 – Proveedores en servicios centralizados o tercerizados:** En este caso, se identifican todos aquellos servicios de proveedores dedicados al procesamiento, traslado o almacenamiento de datos.
- **N8 – Información en conocimiento del personal:** Corresponde a la información que se encuentra en conocimiento de los Recursos Humanos de la entidad.

En el siguiente gráfico se pueden identificar, a modo de ejemplo, cómo se encuentran interrelacionados los subconjuntos de activos de información:

ESQUEMA N°1: Subconjuntos de activos de información



Fuente: Elaboración propia.

1.4.3. Vinculación de los activos de información

Con la clasificación de categorías de activos descripta, se pueden identificar la mayoría de las unidades de información contenidas en las organizaciones. Entre

ellos se puede identificar diversas vinculaciones, por ejemplo, en el caso de analizar un proceso de negocio (N1), se puede observar que existe una dependencia de ese proceso en la documentación existente en papel (N2) e información almacenada (N3) en un aplicativo (N4); asimismo, ese software se encuentra instalado en un equipo informático (N5) y este último alojado en un sitio físico (N6) que recibe servicios de internet de un proveedor (N7).

Resulta importante reconocer a todos los activos de información dado que, si bien estaríamos incluyendo conceptualmente en varios activos la misma información, las vulnerabilidades y las amenazas de cada uno de los activos no son iguales. En este punto, se destaca lo expuesto por (Sallis, Caracciolo, & Rodriguez, 2010), en donde establecen que "*el análisis de vulnerabilidades no sólo es correr herramientas destinadas a tal fin, también deben involucrarse los análisis funcionales necesarias a tal fin de detectar las posibles debilidades en los procesos humanos*."

En esta línea, se destacan algunos estándares internacionales como la IRAM/ISO/IEC 27.002 en donde se especifican los elementos básicos a considerar en la identificación de los activos de información:

> *"Existen muchos tipos de activos, incluyendo:*
>
> *a) información: bases de datos y archivos de data, contratos y acuerdos, documentación del sistema, información de investigaciones, manuales del usuario, material de capacitación, procedimientos operacionales o de soporte, planes de continuidad del negocio, acuerdos para contingencias, rastros de auditoría e información archivada.*

b) activos de software: software de aplicación, software del sistema, herramientas de desarrollo y utilidades;

c) activos físicos: equipo de cómputo, equipo de comunicación, medios removibles y otro equipo;

d) servicios: servicios de computación y comunicación, servicios generales; por ejemplo, calefacción, iluminación, energía y aire acondicionado;

e) personas, y sus calificaciones, capacidades y experiencia;

f) intangibles, tales como la reputación y la imagen de la organización." (International Organization for Standardization / International Electrotechnical Commission, 2013)

En la definición de este estándar internacional, se destacan los archivos de información, activos de software y hardware, servicios, personas y aquellos activos intangibles. La misma será tenida en cuenta cuando se definan las características del sistema de activos de información.

1.5. Conclusiones particulares del capítulo I

Considerando la definición de patrimonio dispuesta por el Dr. Chaves en relación con su movilidad, algunos *"le permiten al ente el desarrollo de su actividad específica o le brindan al ente una estructura permanente para facilitar las mencionadas actividades";* la información cumple con las condiciones para ser considerada como una estructura para el desarrollo de las actividades en las entidades.

Desde la perspectiva de un modelo contable no monetario, y para el reconocimiento eficiente de los datos e información, hay que definir como activo de información a todo elemento que contenga, almacene, procese o transmita información de la entidad bancaria.

Al interpretar la Teoría del propietario, al caso particular de la contabilización de activos de información, se identifica que existe un interés en las entidades que posee la custodia de la información por sobre la titularidad de otras personas físicas y jurídicas. En este planteo, los particulares de los datos serían ajenos a la información ya que los datos solamente corresponderían a la entidad que tiene su custodia.

Asimismo, al analizar la interpretación de la Teoría de la Entidad al caso particular de la contabilización de activos de información, se identifica la existencia de un conjunto de datos que cuya propiedad no es exclusiva de la entidad, sino, que corresponden a otras personas humanas y jurídicas, y en el caso de las entidades financieras, estas ejercen el control real de la información. Por lo tanto, la información existente en las entidades corresponde a dos tipos de titulares, los que son titulares y los que poseen la custodia de los datos. En el contexto de la contabilización de los activos de información se identifica que el objetivo de esta Teoría es el proporcionar datos o información útil a quienes controlan los activos de información, sin dejar de brindarle garantías a los titulares de los mismos.

Con esta última definición y teniendo en cuenta en quien recae la custodia de los datos, se pueden identificar dos clases de activos de información: los que se encuentran en custodia de la organización que se los puede clasificar como:

Procesos (N1); Documentación en papel (N2); Repositorios de archivos y bases de datos (N3); Plataforma de Software (N4); Plataforma de Hardware (N5) o Sitios físicos (N6); y los que se encuentran en custodia de terceras partes se los puede clasificar como Proveedores en servicios centralizados (N7) o información en conocimiento del personal (N8).

Si bien con este tipo de definición y clasificación de activos se estaría identificando a toda la información existente en una entidad, se destaca la existencia de interrelaciones e interdependencias entre unos y otros. Cada activo de información posee características propias con vulnerabilidades y amenazas particulares, por lo tanto, corresponde que sean analizadas en forma individual para efectuar un relevamiento completo de los activos de información en las entidades bancarias.

Capítulo II

2. Identificación de los elementos para la descripción de un Marco conceptual para el tratamiento contable no monetario de los activos de información

2.1. Introducción

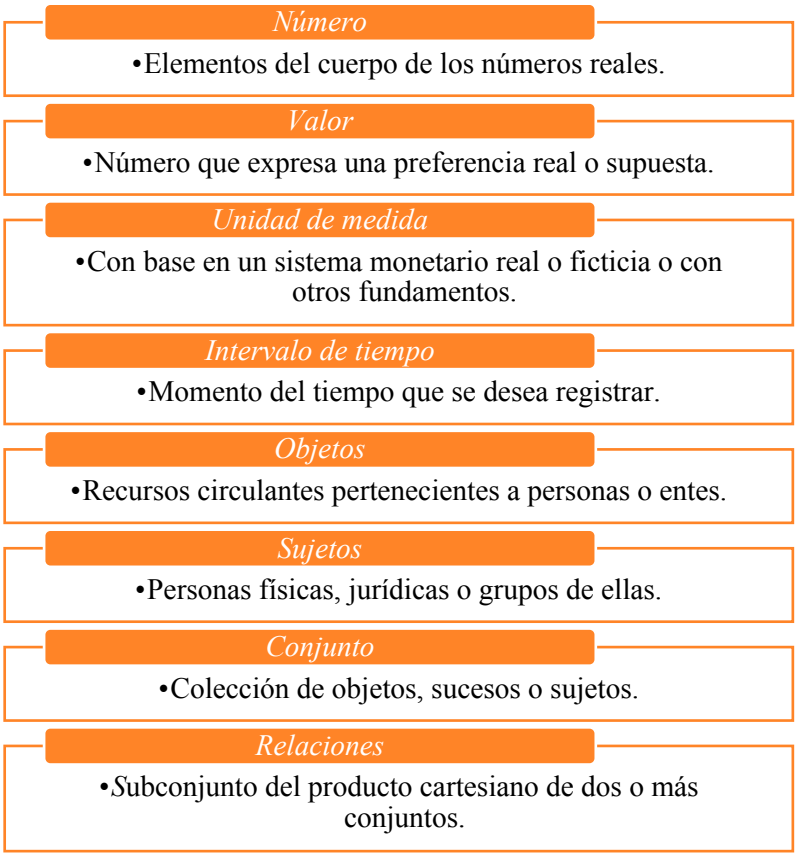
El presente capítulo tiene el objetivo de identificar los elementos para la descripción de un Marco Contable para el tratamiento de los activos de información y como

también se analizarán las hipótesis y las leyes propuestas por los autores en el marco de la presente tesis.

2.2. Bases para identificar a la contabilización de activos de información

El autor Richard Mattessich en su obra "Accounting and analytical methods. Measurement and projection of income and wealth in the micro- and macro-economy." (1964), identifica los siguientes términos primitivos para el desarrollo de un Marco General Contable:

ESQUEMA N°2: Términos primitivos para un Marco General Contable



Fuente: (García Casella & Rodríguez de Ramírez, Elementos para una Teoría General de la Contabilidad, 2011, págs. 25-26)

En base a estas definiciones, los autores (Fronti de García & García Casella, 2009, págs. 58, 59) con el objeto de superar la visión reduccionista y economicista con que se formularon inicialmente, establecieron los siguientes supuestos básicos:

ESQUEMA N°3: Tabla de supuestos básicos en las Ciencias Contables

Supuestos básicos en las Ciencias Contables
Existe un sistema numérico para expresar o medir preferencias (valores) en forma de cantidades monetarias o no monetarias.
Existe un sistema numérico para ordenar, adicionar y medir intervalos de tiempo.
Existe un conjunto de objetos, hechos y personas cuyas características son susceptibles de cambio.
Existe un conjunto de sujetos que tienen relaciones con los objetos, hechos y personas y expresan sus preferencias acerca de ellos.
Existe, al menos, una unidad o entidad cuyas diversas situaciones, en especial frente al cumplimiento de objetivos, se van a describir.
Existe un conjunto de relaciones denominado estructura de la unidad que está representado por un sistema jerarquizado de clases llamado plan de cuentas.

Existe una serie de fenómenos que cambian la estructura y composición de los objetos.
Existen unos objetivos específicos o necesidades de información dadas, las cuales deben ser cubiertas por un concreto sistema contable. La elección de las reglas e hipótesis específicas depende del propósito o necesidad señalados.
Existe un conjunto de reglas alternativas que determinan qué valores deben ser utilizados en cada registración.
Existe un conjunto de reglas alternativas que determinan el sistema de clasificación de las cuentas.
Existe un conjunto de reglas alternativas que determinan los datos de entrada y el grado de agregación de estos datos.
Fuente: (García Casella C. , Corrientes doctrinarias actuales en contabilidad, 1992)

Para ampliar el enfoque anterior, (García Casella C. , El problema del uso de modelos en la contabilidad, 2002) presenta los siguientes lineamientos en materia contable:

ESQUEMA N°4: Lineamientos básicos en materia contable propuestos por García Casella

Lineamientos básicos en materia contable
La contabilidad sería no solo para empresas, sino también para individuos, organismos públicos, entidades sin fines de lucro, en los que hay que tener en cuenta ciertos aspectos que tienen que ver con lo social.
La contabilidad no sólo tiene que ocuparse de la cuantificación de los patrimonios, sino también del cumplimiento de los objetivos del ente.
La contabilidad se debe expresar no solo en términos monetarios, sino que debe incluir además los no monetarios.
La contabilidad debe estar formada por información histórica y predictiva.
La contabilidad debe aplicar métodos estadísticos a la obtención y procesamiento de datos para el análisis de la realidad.
La contabilidad no solo tiene que cumplir requerimientos legales y fiscales, sino que tiene que servir a la toma de decisiones; y ebe informar de muchas cosas más que patrimonio
Fuente: **(García Casella C. , 2002)**

En esta línea, los autores Eutimio Mejía Soto, Carlos Alberto Montes Salazar y Gloria Cecilia Dávila, consideran que:

> "*Se sustenta en el pensamiento de Richard Mattessich pero corrigiendo el carácter y sesgo economicista y empresarial. Si bien la teoría general contable de Mattessich pretende ser universal y polivalente, la descripción y la definición de los supuestos, axiomas y teoremas reducen el saber contable; García-Casella percibe esta situación, lo que le permite reformular estas estructuras conceptuales tendiendo a una concepción más universal y amplia de la contabilidad*." (Introducción a la propuesta contable de García-Casella, 2011)

En base a estas definiciones, a continuación se analizarán los elementos necesarios del Marco Contable General para contrastar, analizar y describir otros Marcos Conceptuales particulares, que en la presente investigación están orientados a un Marco Conceptual para los activos de información en entidades bancarias.

2.3. Características del fenómeno observado en la presente investigación

Como se indicó en el capítulo precedente, en las entidades financieras se observa la identificación de información en diversas formas y con un tratamiento único que no se manifiesta en otro tipo de entidades.

En el estudio de casos llevado a cabo, se observó la registración de activos de información bajo características propias de identificación, análisis, seguimiento, medición, control y auditoría.

A continuación, se detallarán los elementos a identificar en la investigación desarrollada en la presente tesis.

2.4. Bases teóricas contables para el desarrollo de un Marco Conceptual para la contabilización de activos de información en entidades bancarias

Para el análisis y contrastación de los Modelos Contables resulta necesario identificar el Marco Conceptual aplicable. Como indica el autor Walter René Chiquiar, en su artículo titulado: Aproximación a un marco conceptual de la contabilidad no monetaria (aplicada a la contabilidad ambiental):

> "*La Contabilidad posee un Marco Conceptual General (MCG) aplicable de manera amplia al dominio de su universo, mas a él se agregan otros marcos conceptuales específicos de cada una de áreas contables, los cuales deben ser consistentes y congruentes con el MCG."* (2009, pág. 21)

En esta línea de investigación, se destaca la visión de los directores del proyecto de investigación: Carlos Luis García Casella, Luisa Fronti de García y María del Carmen Rodríguez de Ramírez cuyas conclusiones de se publicaron en el libro: *Elementos para una teoría general de la contabilidad* (2001), en donde identifica los

siguientes elementos necesario para la construcción del Marco Conceptual Contable General:

ESQUEMA N°5: Elementos que son relevantes para la construcción del Marco Conceptual Contable General

Elementos para el Marco Conceptual Contable General
Naturaleza o estatus epistemológico de la contabilidad
Sistemas contables
Medición
Personas o sujetos de la actividad contable
Relaciones de la contabilidad con otras disciplinas
Segmentación o unidad contable absoluta
Dominio o universo del discurso contable
Modelos en teoría general contable
Fuente: **(García Casella, Fronti de García, & Rodríguez de Ramírez, 2001)**

Los citados autores desarrollaron hipótesis y propusieron leyes para cada uno de los problemas identificados como Elementos para una TGC, a continuación, se detallará como se analizarán en los siguientes capítulos.

2.5. Contrastación de las hipótesis y leyes por los autores Carlos Luis García Casella, Luisa Fronti de García y María del Carmen Rodríguez de Ramírez

Como se indicó en el cuerpo introductorio, el tipo de diseño de investigación llevado a cabo en la tesis es un estudio de casos, ya se desarrolla una indagación profunda y detallada del fenómeno planteado.

Para este caso, es necesario la descripción de los elementos que conforman un modelo contable específico para el tratamiento de los activos de información.

En los siguientes capítulos se tomarán cada uno de los problemas identificados por los autores para describir el fenómeno en las entidades bancarias y en la conclusión se compararán con las leyes teóricas propuestas para cada uno de ellos.

2.6. Conclusiones particulares del capítulo II

Para la descripción de un Marco Teórico particular relacionado con los activos de información, resulta indispensable partir de las bases teóricas del Marco Conceptual Contable General.

Para la contrastación de los mismos, se han tomado los elementos descriptos por García Casella y equipo (2001), los cuales son: Naturaleza o estatus epistemológico de la contabilidad, Sistemas contables, Medición, Personas o sujetos de la actividad contable, Relaciones de la contabilidad con otras disciplinas, Segmentación o unidad contable absoluta, Dominio o universo del discurso contable y Modelos de la Teoría General Contable.

En los siguientes capítulos de la presente tesis, se propone describir el sistema contable de activos de información; identificar a las personas y sujetos de la actividad contable y plantear un modelo teórico de valorización de los activos de información. Asimismo, realizar un relevamiento de las mejores prácticas y estándares relacionados con el control de los activos de información en custodia de los entes, en conocimiento de los recursos humanos y en posesión de terceras partes.

Capítulo III

3. Dominio del discurso contable de activos de información

3.1. Introducción

En este capítulo se analizará el dominio del discurso contable en el tratamiento de los activos de información desde la perspectiva del segmento no monetario. Como se indicó precedentemente, para ello se toma como eje principal la hipótesis del primer problema sobre el discurso contable identificado por los doctores: Carlos Luis García Casella, Luisa Fronti de García y María del Carmen Rodríguez de Ramírez:

> *"Integran el dominio o universo del discurso contable todos los componentes, ya sean objetos, hechos, personas o reflexiones que intervienen en la interrelación informativa sobre actividades, hechos, transacciones socioeconómicas que procuran medir el cumplimento de metas en diversos niveles dentro de las organizaciones sociales y entre las mismas."* (2001)

Para poder identificar el dominio o universo del discurso contable en el tratamiento de los activos de información en el ámbito bancario, se necesitan, como indica la hipótesis de los autores, identificar a todos los elementos que lo componen. A continuación, se describirán las bases necesarias para el análisis del fenómeno observado.

3.2. Identificación de los elementos del dominio del discurso contable

Para el fenómeno observado, descripto como la contabilización de los activos de información como un segmento contable no monetario, se identificaron y analizaron los siguientes elementos en el estudio de casos relevados en la entidad bancaria:

ESQUEMA N°6: Elementos identificados del dominio del discurso contable de activos de información

Elementos necesarios según los autores CLGC, LFG y MCRDM	¿Se observó el elemento en el estudio de casos?	Resultado del estudio de casos en entidades Bancarias en el tratamiento de los activos de información
1- Informes Contables de Uso Externo a los emisores.	SI	Existen informes de uso externo a los emisores relacionados al inventario de activos de la información, las bases de datos utilizadas en la entidad y la utilización de proveedores críticos, como presentados en el BCRA y la AAIP.
2- Personas y grupos de personas emisoras de los diversos informes contables.	SI	En las entidades bancarias se identifican grupos de personas desarrollando informes internos y externos sobre los activos de información.

3- Personas revisoras que opinan sobre la calidad de los informes contables.	SI	En los casos observados se identifican revisores de la calidad de los informes internos y externos sobre los activos de información.
4- Personas o grupos de personas usuarias o destinatarias de los diversos informes contables.	SI	En las entidades bancarias se identifican grupos de personas usuarias de los informes de activos de información.
5- Personas o grupos de personas reguladoras de los distintos informes contables.	SI	En el sector bancario se encuentran sectores reguladores (como el BCRA y la AAIP) de los informes internos y externos sobre los activos de información.
6- Microsistemas Contables propios de cada ente.	SI	En las entidades bancarias se observa un microsistema contable de activos de información.
7- Macrosistemas Contables definidos	SI	En las entidades públicas del ámbito de la Ciudad Autónoma de Buenos

en ciudades, países, regiones, o en tipos de actividad o en clases diferentes de organizaciones.		Aires se encuentra definido un Macrosistema contable de activo de información, con el objetivo de identificar las infraestructuras críticas. Y en el caso de la AAIP existe un inventario con todas las bases de datos registradas a nivel nacional.
8- Modelos contables necesarios para determinar variables relevantes en diversas situaciones.	SI	En el fenómeno estudiado, se identifica un modelo contable para los activos de información.
9- Informes contables de uso interno en cada ente.	SI	En el ámbito bancario se identifican informes de uso interno.
10- Informes contables de organismos gubernamentales.	SI	En el ámbito bancario de la CABA se identifican informes de activos de información a nivel gubernamental.

11- Informes contables macrosociales.	SI	Se identifican informes contables a nivel del BCRA y la AGCABA.
12- Informes contables microsociales.	SI	Se identifican informes contables microsociales internos y externos sobre los activos de información.
13- Segmentos contables.	SI	En el caso se puede observar que la contabilización de activos de información constituye parte del segmento contable no monetario.

En base el estudio de casos realizado, en los siguientes capítulos se describirán los hallazgos de cada uno de los elementos necesarios para la formalización de un Marco Contable Alternativo.

3.3. Conclusiones del capítulo III

A modo de conclusión, se contrastarán cada una de las leyes teóricas para el primer problema sobre el dominio del discurso contable de los activos de información.

ESQUEMA N°7: Contrastación del dominio del discurso contable

Leyes sobre el dominio del discurso contable enunciadas por los autores CLGC, LFG y MCRDM.	Contrastación de las leyes en el contexto de la contabilización de activos de información.
1. Las personas y las entidades siempre dedican una parte de sus energías o esfuerzos a lograr objetivos no económicos.	En la contabilización de los activos de información se ha identificado que las personas y entidades asignan recursos para el cuidado y control de los datos.
2. Las personas y las organizaciones no pueden decidir en base exclusivamente de datos del pasado y del presente, necesitan datos del futuro.	En la contabilización de los activos de información se ha identificado que en la registración se utilizan datos históricos, del presente como también pronósticos para preparar medidas de protección ante futuros ataques.
3. Las cuestiones patrimoniales no son las únicas que interesan a los decididores individuales y a los decididores de las organizaciones.	En la contabilización de los activos de información se ha identificado un interés por parte de las personas en proteger el perímetro de seguridad, fuga de información y ataques cibernéticos entre otros.
4. La Contabilidad produce informes contables pero no se limita a ellos	En la contabilización de los activos de información se ha identificado otros

en su dominio o universo del discurso.	tipos de informes como los relacionados a la ley de datos personales, informes de capacitación e informes internos exigidos por los organismos de control.
5. Las personas humanas y las organizaciones de personas humanas como no actúan exclusivamente para obtener ganancias necesitan que la Contabilidad les provea de informes que midan cumplimento de objetivos de distinto tipo y no solamente económicos.	En la contabilización de los activos de información se provee distintos tipos de informes para dar cumplimento los objetivos propuestos por la gestión.
6. La Contabilidad recibe aportes de la Economía pero éstos no bastan para resolver todos los problemas que la Contabilidad tiene a su cargo.	La contabilización de los activos de información no contradice la ley propuesta de la TGC.
7. Los sistemas contables particulares, que producen Estados Contables son solamente una parte	En la contabilización de los activos de información se ha identificado un sistema de contabilización de activos de información.

del dominio o universo del discurso contable.	
8. Las prácticas contables generalmente, aceptadas o no, no son principios sino realidades que integran el contenido de la Contabilidad pero cohabitan con muchos otros elementos.	La contabilización de los activos de información no contradice la ley propuesta de la TGC.
9. La Contabilidad abarca tareas de control económico como una pequeña parte del dominio o universo del discurso contable.	En la contabilización de los activos de información se ha identificado tareas de control para cada uno de los tipos de datos identificados.
10. La Contabilidad se ocupa de temas que proveen diversas disciplinas, pero por ello no depende de sus respectivas teorías sustentadoras.	En la contabilización de los activos de información se ha identificado que se relaciona con otras disciplinas como la tecnología y la seguridad de la información convirtiéndose en una herramienta para la gestión.
11. La Contabilidad estudia todos los fenómenos que ocurren en las organizaciones con la intención de	En la contabilización de los activos de información se ha identificado su rol de informar para la toma de decisiones,

ir brindando información sobre cumplimento de metas organizacionales no exclusivamente económicas y no exclusivamente en forma cuantitativa.	metas, políticas de gestión y no solamente para metas económicas.
12. La Contabilidad no está vinculada exclusivamente al principio de dualidad: hay acciones humanas en las organizaciones que no corresponden a ese principio y son materia de la disciplina.	En la contabilización de los activos de información no está vinculada con el principio de la dualidad económica.
13. La Contabilidad tiene un campo amplio de actuación que no se limita a considerar exclusivamente a las transacciones.	En la contabilización de los activos de información se ha identificado que no se limita a registrar transacciones.
14. Aunque la Contabilidad tiene relación con la Teoría de la Medición, es independiente de ella en muchos aspectos de su actuación.	En la contabilización de los activos de información se ha identificado formas específicas de clasificar la información, pero existen varios criterios.

15. No es posible expresarlas relaciones y mediciones contables exclusivamente en términos monetarios.	En la contabilización de los activos de información las registraciones de eventos no son en términos monetarios.
16. El dominio o universo del discurso contable abarca hechos y actos del pasado, del presente y del futuro.	En la contabilización de los activos de información se registran eventos del pasado, del presente y se estiman en el futuro.

Como se puede observar en el cuadro precedente, la contabilización de los activos de información se observan los siguientes elementos del dominio contable en el ámbito bancario:

1- Informes sobre activos de información de Uso Externo a los emisores.

2- Grupos de personas emisoras de los diversos informes sobre activos de información internos y externos.

3- Personas revisoras o que ejercen el rol de control de los informes sobre activos de información.

4- Personas o grupos de personas usuarias o destinatarias de los diversos informes contables.

5- Grupos de personas reguladoras de los distintos informes contables de activos de información.

6- Microsistemas Contables de activos de información.

7- Macrosistemas Contables de activos de información.

8- Elementos para la formalización de un modelo contable para los activos de información.

9- Informes contables de activos de información de uso interno.

10- Informes contables de activos de información de organismos gubernamentales.

11- Informes contables de activos de información macrosociales.

12- Informes contables de activos de información microsociales.

13- Segmentos contables no monetario para los activos de información.

Capítulo IV

4. Naturaleza epistemológica de la contabilización de activos de información

4.1. Introducción

La Contabilidad como disciplina ha sido definida epistemológicamente por los investigadores a lo largo de la historia como: Ciencia, Arte, Técnica, Tecnología y Tecnología Social. Cada definición se fundamentó partiendo de la observación empírica basada en la descripción de la contabilidad, lo que posibilitó la descripción de diferentes segmentos contables.

En esta línea, el segundo problema identificado para los modelos contables radica en la naturaleza epistemológica de la contabilidad, en donde resulta necesario definirla para poder definir una Teoría General Contable aplicable al resto de los segmentos existentes, sean monetarios o no.

Los citados autores, Carlos Luis García Casella, Luisa Fronti de García y María del Carmen Rodríguez de Ramírez, concibieron la hipótesis que la "*Contabilidad es una Ciencia factual, cultural y aplicada*", en base a la clasificación de las Ciencias propuestas por Mario Bunge.

El presente capítulo tiene por objetivo identificar la definición de contabilidad, segmentos y los elementos básicos para el desarrollo de un Modelo Conceptual Contable.

4.2. Definición actual de la disciplina contable

A continuación, se destacan las definiciones de Contabilidad más relevantes para la presente investigación. La definición difundida por la American Accounting Association, establece que:

> *"…La Contabilidad es un proceso de medición y comunicación que puede ser aplicado a una variedad de temas. La mayoría de las aplicaciones han tratado sobre recursos económicos (así definidos tradicionalmente) y la mayor parte de la discusión actual se orienta a estas aplicaciones. No obstante, como se sugiere en mayor profundidad en el Capítulo V, la*

Contabilidad no tiene por qué estar confinada a dicho objeto", traducido por (Chiquiar W. R., 2009).

En la citada definición se plantea una visión de la contabilidad abocada a diversos segmentos y propósitos, desencasillándola del segmento financiero. En la misma línea, el autor Walter Chiquiar manifiesta que:

> "*La Contabilidad brinda información sobre la circulación de objetos, hechos y personas atribuibles a un ente. Dicha circulación determina un flujo continuo sobre el cual se hacen observaciones puntuales a los efectos de emitir información. La información requerida está vinculada con la necesidad del proceso de toma de decisiones con impacto en el futuro.*" (Aproximación a un marco conceptual de la contabilidad no monetaria (aplicada a la contabilidad ambiental), 2009, pág. 122)

Considerando la definición de Contabilidad propuesta por García Casella en la que enuncia que "*es una ciencia factual, cultural, aplicada, que se ocupa de las interrelaciones entre los componentes de los hechos informativos de todo tipo de ente*" (Naturaleza de la Contabilidad, 1997) y que los sistemas contables concretos "*responderían a los Modelos Contables Alternativos que pueden elaborarse para satisfacer intereses de usuarios en sus respectivas decisiones.*"

Al identificarse qué debería esperarse de esta disciplina, el autor cita la siguiente traducción de Iselin en donde establece que *"el campo de la Contabilidad debería abarcar cualquier tipo de información necesaria para la toma de decisiones sobre las entidades, es decir, retrospectiva, presente y prospectiva, monetaria y no monetaria; económica y no económica; cuantitativa y no cuantitativa; la información*

debería proporcionarse de acuerdo a las necesidades de los decisores." traducido por (García Casella, Fronti de García, & Rodríguez de Ramírez, 2001, pág. 26). Esta definición es trascendental dado que se identifican múltiples líneas para investigar a la contabilidad y no solamente desde la problemática financiera.

La contabilidad como disciplina, fue conceptualizada por el Dr. Carlos Luís García Casella, quien la define como:

> "*una ciencia aplicada factual cultural que se ocupa de la descripción cuantitativa y de la proyección de la existencia y circulación de los objetos diversos en cada ente u organización social, en vista al cumplimiento de sus metas a través de un método basado en un conjunto de supuestos básicos* [...]". (García Casella C. L., Método Científico para las Investigaciones en General, 1995)

En esta línea, se concuerda con el autor Goldberg en donde establece que *"atar a la Contabilidad irrevocablemente a las ocurrencias financieras es demasiado restrictivo y no se compadece con los hechos y los procedimientos contables tal como se llevan a cabo en la actualidad"* traducido por (García Casella, Fronti de García, & Rodríguez de Ramírez, 2001, pág. 25).

4.3. Su vinculación con contabilización de los activos de información

En el análisis teórico de la contabilización de los activos de información resulta fundamental encuadrar a la disciplina como ciencia aplicada. A continuación, se analizarán las leyes propuestas por los autores para la naturaleza epistemológica:

ESQUEMA N°8: Contrastación de la naturaleza epistemológica de la contabilidad

Leyes sobre la naturaleza epistemológica de la contabilidad enunciadas por los autores CLGC, LFG y MCRDM.	Contrastación de las leyes en el contexto de la contabilización de activos de información.
1. La Contabilidad no puede ubicarse entre las artesanías ni entre las Bellas Artes porque responde a abstracciones teóricas que describen y norman la actividad contable con métodos que tienen rigor científico.	La contabilización de los activos de información no contradice la ley propuesta.
2. La Contabilidad incluye en su dominio técnicas repetitivas que	En la contabilización de los activos de información se identifican técnicas

deben basarse en desarrollos teóricos y -mejor aún- en modelos abstractos que representan las variables relevantes de cada fenómeno.	específicas de registración y se pueden identificar a cada uno de los elementos para describir un modelo contable alternativo.
3. La Contabilidad tiene principios o fundamentos propios que hacen que sus actividades se basen en propuestas independientes y válidas para el mejoramiento del servicio contable.	La contabilización de los activos de información no contradice la ley propuesta. La misma posee fundamentos propios como la registración y medición de los activos.
4. La Contabilidad incluye -esencialmente- una tradición de investigación que se perpetúa en las fuertes relaciones de información que tienen entre sí los investigadores contables.	La contabilización de los activos de información no contradice la ley propuesta de la TGC.
5. Los organismos nacionales e internacionales toleran y -mejor aún apoyan y estimulan la investigación contable.	La contabilización de los activos de información no contradice la ley propuesta de la TGC. Existen diversos proyectos relacionados con la ciberseguridad.

6. La actividad contable se refiere a cosas cambiantes, con una teoría del conocimiento realista crítica y una ética de la libre búsqueda de la verdad.	La contabilización de los activos de información no contradice la ley propuesta de la TGC.
7. La Contabilidad tiene un trasfondo formal que consiste en una colección de teorías lógicas y matemáticas al día, en lugar de ser vacía o de estar formada por teorías formales anacrónicas.	La contabilización de los activos de información no contradice la ley propuesta de la TGC.
8. La Contabilidad utiliza una colección de datos, hipótesis y teorías al día confirmadas (aunque no incorregibles) obtenidas en otros campos de investigación relevantes a ella.	La contabilización de los activos de información no contradice la ley propuesta de la TGC.
9. La Contabilidad es una ciencia que se ocupa exclusivamente de problemas cognoscitivos referentes a la naturaleza de los miembros que componen su	La contabilización de los activos de información no contradice la ley propuesta de la TGC.

dominio y de problemas concernientes a los demás componentes que hacen que sea ciencia.	
10. La Contabilidad tiene un fondo de conocimiento compatible con los de otras disciplinas y reúne lo obtenido por los investigadores científicos de la Contabilidad en tiempos anteriores.	La contabilización de los activos de información no contradice la ley propuesta de la TGC
11. La Contabilidad posee múltiples paradigmas que conviven y fructifican en teorías.	La contabilización de los activos de información no contradice la ley propuesta de la TGC.

Capítulo V

5. Vinculación de la contabilización de los activos de información y otras disciplinas

5.1. Introducción

El tercer problema por analizar es la relación de la contabilidad con otras disciplinas, los citados autores: Carlos Luis García Casella, Luisa Fronti de García y María del Carmen Rodríguez de Ramírez, manifestaron que:

"La Contabilidad es una ciencia independiente, con interrelaciones con otras ya que algunas zonas de su objeto de estudio son concurrentes para otras disciplinas.

La relación de la Contabilidad con la Economía, la Administración, la Estadística, el Derecho y la Matemática es de mutua interrelación, sin dependencia" (2001).

En la presente investigación, las disciplinas más vinculadas con la contabilización de los activos de información es la tecnología y la seguridad de la información. El objetivo del presente capítulo es identificar su relación y su aporte a la Teoría General Contable.

5.2. Concepto de Seguridad de la Información y su vinculación con la contabilidad

La Real Academia Española establece que seguridad es la cualidad de seguro, es decir "*estar libre y exento de todo daño peligro o riesgo"* (RAE, 2017). En tecnología de la información, la seguridad entendida según la citada definición es prácticamente imposible de conseguir, *"por lo que se tiende más al concepto de fiabilidad; entendiéndose a un sistema seguro como aquel que se comporta como se espera de él."* (Gómez López, 2010)

En los sistemas informáticos, ya sean sistemas operativos, de servicios o aplicaciones, se dice que son seguros si cumplen con las siguientes características:

- Confidencialidad: Requiere que la información sea accesible (usarla, leerla o escucharla) sólo para las personas autorizadas.

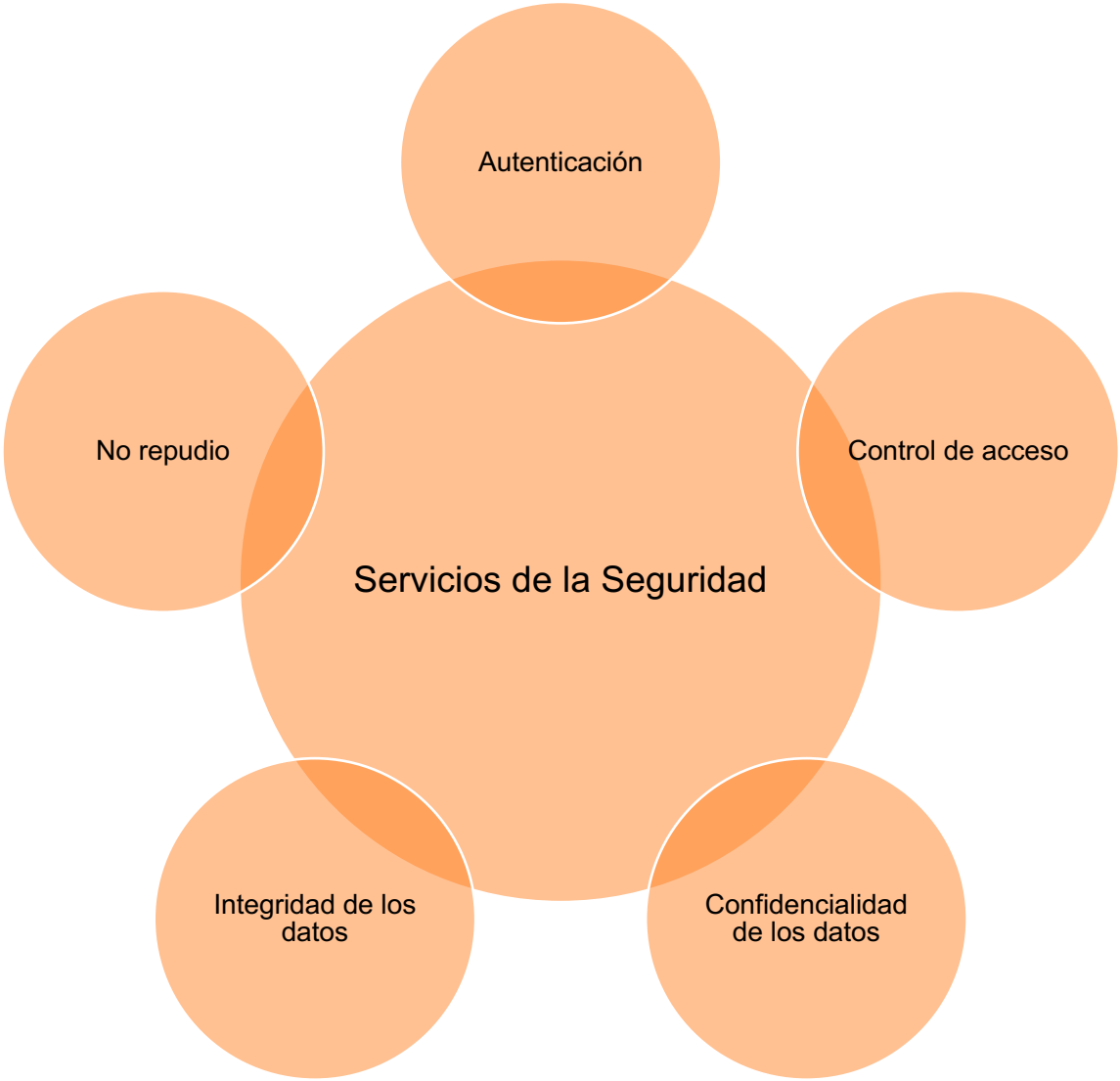
- Integridad: Requiere que la información sólo pueda ser modificada por las entidades autorizadas, asegurando que la información con la que se trabaja sea completa y precisa y poniéndole énfasis en la exactitud tanto en su contenido como en los procesos involucrados en su procesamiento.

- Disponibilidad: Requiere que los recursos del sistema informático estén disponibles para los usuarios y las entidades autorizadas cuando se los necesiten.

Estos conceptos se relacionan con el de Criptografía que *"estudia, entre otros temas, los métodos de encriptación, y el criptoanálisis de las técnicas para intentar quebrarlos. La Criptografía consiste en un conjunto de técnicas al servicio de la seguridad informática y no debe confundirse con ella."* (Scolnik, 2014)

Estos tres requisitos son los básicos, pero según Gustavo Aldegani, el paradigma actual de la seguridad de la información incluye además de los citados principios a la "*Verificación de la Identidad Digital y Registro de sus acciones, Confiabilidad de Navegación, y Prevención de pérdidas de datos*" (Aldegani, 2019). Por lo tanto, se pueden identificar los siguientes servicios asociados a la Seguridad de la Información:

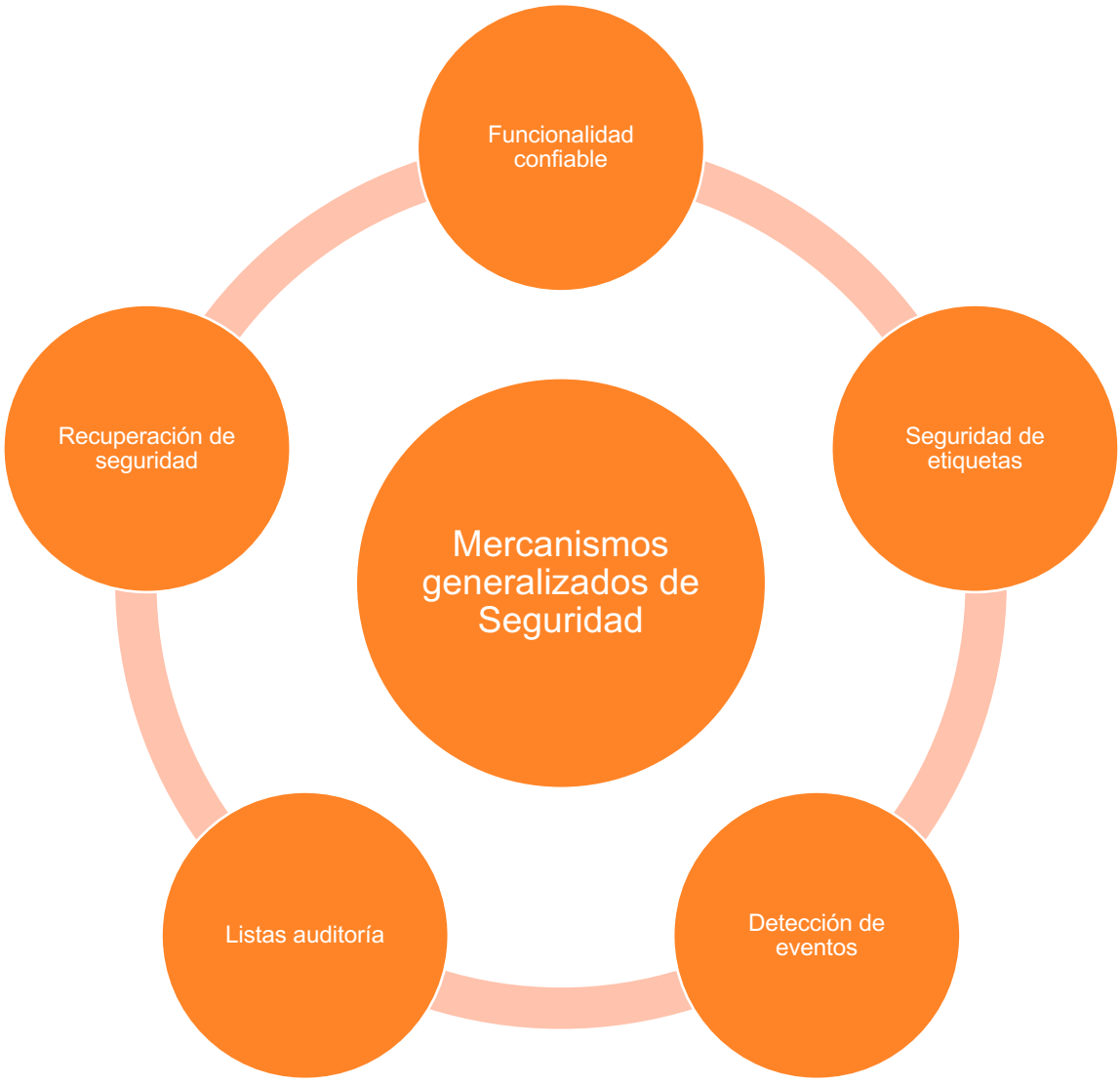
ESQUEMA N°9: Servicios asociados a la Seguridad de la Información



Fuente: Security Services (X.800)[x] (Kahate, 2019)

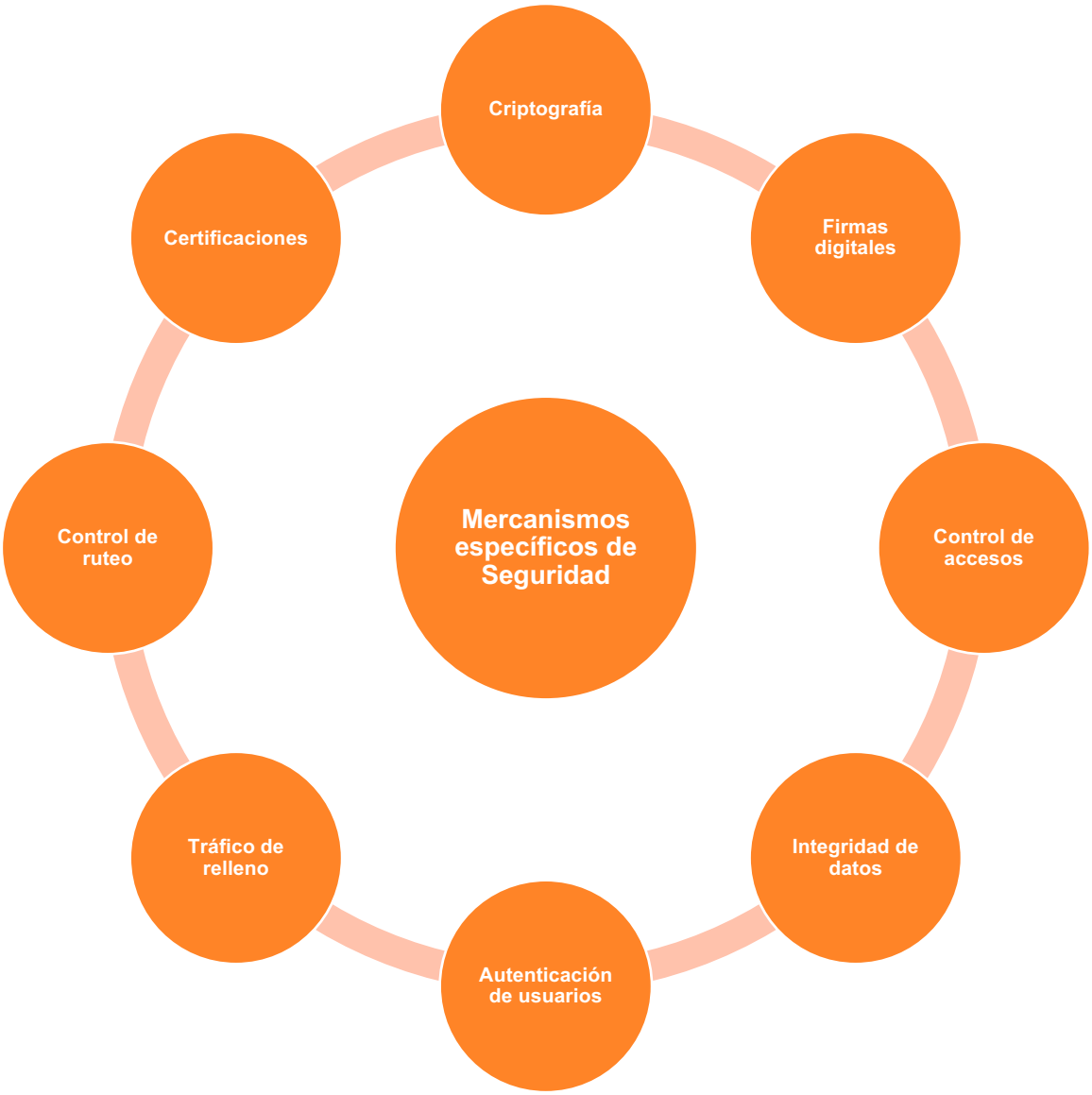
De los que se pueden definir y relacionar los siguientes mecanismos específicos y particulares al servicio de la seguridad de la información como disciplina:

ESQUEMA N°10: Mecanismos generalizados de seguridad



Fuente: Security Mechanisms (X.800) (Stallings, 2016)

ESQUEMA N°11: Mecanismos específicos de seguridad



Fuente: Security Mechanisms (X.800) (Stallings, 2016)

Cada uno de estos conceptos conforman básicamente todos los mecanismos específicos y generales que forman parte de la Seguridad de la Información. Cada uno de ellos impacta en el uso, procesamiento y acceso de los datos existentes en

las entidades. A continuación, se los relacionarán con los requisitos de la información contable.

5.3. Requisitos de la información contable presente en el marco conceptual

En la Resolución Técnica N°16, denominada Marco Conceptual de la Información Contable de la Federación Argentina de Consejos Profesionales en Ciencias Económicas (FACPCE, 2011), se establece que, para cumplir con su finalidad, la información contenida en los estados contables debe reunir los requisitos enunciados a continuación:

ESQUEMA N°12: Requisitos de la Información contenida en los Estados Contables	
Pertinencia (atingencia)	
Confiabilidad (credibilidad)	- Aproximación a la realidad
	- Esencialidad (sustancia sobre forma)
	- Neutralidad (objetividad o ausencia de sesgos)
	- Integridad
Verificabilidad	
Sistematicidad	

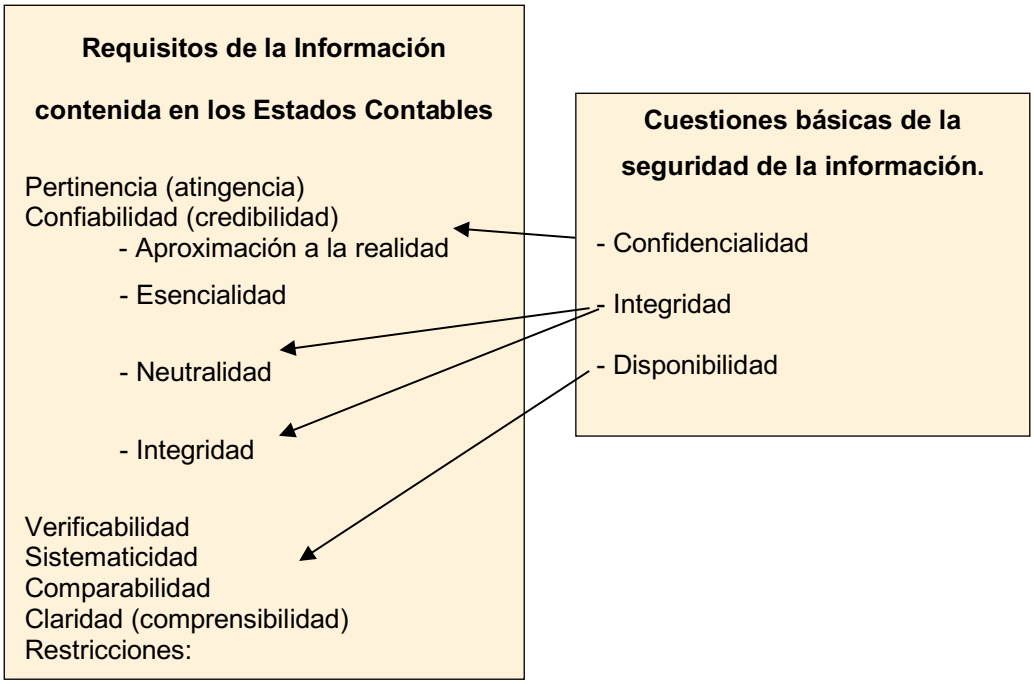
Comparabilidad
Claridad (comprensibilidad)
Consideraciones sobre las restricciones que condicionan el logro de las cualidades recién indicadas:
Oportunidad
Equilibrio entre costos y beneficios
Impracticabilidad
Elaboración propia. Fuente: (FACPCE, 2011)

La contabilidad como campo de conocimiento toma conceptos de otras disciplinas, como la Administración, el Derecho y la Matemática entre otras. En este contexto, la "Tecnología y Seguridad de la Información" debería contemplarse como una de ellas, al contribuir con el cumplimiento de los requisitos de la información contable.

Teniendo en cuenta los citados principios básicos de la seguridad de la información (integridad, confidencialidad y disponibilidad), se puede establecer su contribución al optimizar los requisitos de la información contable, convirtiéndose en el principal sostén del sistema contable en soporte tecnológico.

En el siguiente esquema se plantean los conceptos de la Seguridad de la Información que contribuyen al cumplimiento de los requisitos de la información contable.

ESQUEMA N°13: Aportes de la Seguridad de la Información a la Contabilidad



Fuente: Elaboración propia.

El autor de la presente tesis destaca la definición de Teoría Contable publicada por la American Accounting Association en 1966, en donde se establece que:

> "*Nosotros definimos "teoría" como un conjunto consistente de principios hipotéticos, conceptuales y pragmáticos formando un marco de referencia general para un campo de estudio.*
>
> *Extensión de la Teoría Contable:*
>
> *Debido a los cambios en la tecnología y los avances en el conocimiento de la conducta humana, el alcance y los métodos de la contabilidad están cambiando y se espera que continúen cambiando (…). Las principales áreas en las que están ocurriendo cambios, que pueden influir en la contabilidad del futuro, son percibidas como incluyendo:*

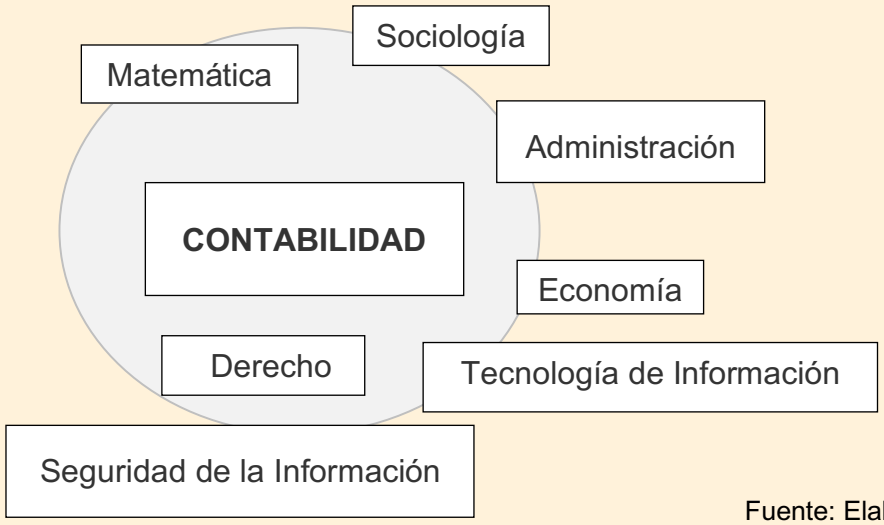
- *Conocimiento de los procesos de decisión.*
- *Conocimiento de las conductas humanas.*
- *Tecnologías de la computación y el diseño de sistemas.*
- *Técnicas de medición y teoría de la información.*"

(García Casella & Rodríguez de Ramírez, Elementos para una Teoría General de la Contabilidad, 2011)

En el año 2020, se han podido corroborar empíricamente los cambios sufridos en la disciplina contable por factores tecnológicos, normativos, legales, como también de índole social.

Al considerar que la Contabilidad toma conceptos de otras disciplinas, se propone incluir a la Seguridad de la Información como una de las nuevas disciplinas influyentes en la contabilidad al considerar su innegable contribución al cumplimento de los requisitos y el resguardo de la información contable.

ESQUEMA N°14: Disciplinas influyentes en la Contabilidad



Fuente: Elaboración propia.

Otro factor por destacar es el planteo de la Seguridad de la Información como una disciplina separada de la Tecnología de la Información, *"ya que la misma incluye otros conceptos que no son específicamente tecnológicos como por ejemplo la Seguridad Física"* (Escobar, 2013).

Como se describió precedentemente, los diferentes activos de información existentes en las entidades bancarias que pueden identificarse son: Procesos (N1); Documentación en papel (N2); Repositorios de archivos y bases de datos (N3); Plataforma de Software (N4); Plataforma de Hardware (N5) o Sitios físicos (N6), Proveedores en servicios centralizados (N7) e información en conocimiento del personal (N8). En cada uno de ellos, la Seguridad de la información impacta como se puede observar en el siguiente cuadro:

ESQUEMA N°15: Elementos del sistema de activos de información contable y la Seguridad de la Información		
Sistema Contable de activos de información	Elementos	Seguridad de la Información
	Procesos (N1);	Mejores prácticas de control interno
	Documentación en papel (N2)	Seguridad Física
	Repositorios de archivos y bases de datos (N3)	Seguridad en los Aplicativos y Bases de Datos
	Plataforma de Software (N4)	Seguridad en los Aplicativos

	Plataforma de Hardware (N5)	Seguridad lógica y Física
	Sitios físicos (N6)	Seguridad Física
	Proveedores en servicios centralizados (N7)	Seguridad en los Sistemas Operativos o Software de base
	Información en conocimiento del personal (N8).	Ética y compromiso con la organización
Fuente: Elaboración Propia.		

Por todo lo expuesto, el objetivo de los siguientes capítulos consiste en analizar la contribución de la Seguridad de la Información en los diferentes activos de información existentes en las entidades bancarias:

- ✓ Legislación nacional vigente.
- ✓ Resguardo de la información contable.
- ✓ Estándares y mejores prácticas en el control.
- ✓ Disposiciones y resoluciones de los organismos de control.

5.4. Conclusiones preliminares del capítulo V.

La Contabilidad analizada como disciplina es influida por numerosas ciencias básicas y aplicadas, que le aportan nuevas herramientas y características a cumplir para garantizar los requerimientos de la información de los diferentes grupos de interés.

En este análisis, la “Seguridad de la Información” debe contemplarse como una disciplina influyente sobre la contabilidad al contribuir con el cumplimiento de los requisitos de la información contable establecidos en el Marco Conceptual; dado que brinda los mecanismos específicos y generales para garantizar el cumplimiento de los principios básicos de la seguridad, impactando en cada uno de los elementos que componen el sistema contable de activos de las entidades bancarias: Procesos (N1); Documentación en papel (N2); Repositorios de archivos y bases de datos (N3); Plataforma de Software (N4); Plataforma de Hardware (N5) o Sitios físicos (N6), Proveedores en servicios centralizados (N7) e información en conocimiento del personal (N8).

Asimismo, la gestión de la Seguridad tiene efectos en cada uno de ellos, como en la administración la seguridad de los aplicativos y sistemas operativos, la seguridad física y la concientización del personal, entre otros.

De esta manera, la Seguridad de la Información se convierte en el principal sostén de los requisitos a satisfacer por los Sistemas de Información y no puede concebirse en el Siglo XXI una organización que prescinda de las bondades que ella brinda.

A continuación, se analizarán las leyes propuestas por los autores para la relación de la contabilidad y otras disciplinas:

ESQUEMA N°16: Contrastación de la relación de la contabilidad y otras disciplinas

Leyes sobre la relación de la contabilidad y otras disciplinas enunciadas por los autores CLGC, LFG y MCRDM.	Contrastación de las leyes en el contexto de la contabilización de activos de información.
1. Las personas y las entidades siempre dedican una parte de sus energías o esfuerzos a lograr objetivos no económicos.	En la contabilización de los activos de información se contribuye al logro de objetivos no económicos.
2. Las personas y las organizaciones para decidir necesitan datos del futuro, y no en base exclusiva del pasado y del presente.	En la contabilización de los activos de información se presenta información proyectada para el armado de escenarios en los planes de continuidad operativa de las entidades.
3. A los decididores individuales y a los decididores de las	En la contabilización de los activos de información se informan eventos y

organizaciones les interesan otras cuestiones además de las cuestiones patrimoniales.	situaciones que no tienen relaciones con las patrimoniales.
4. La Contabilidad en su dominio o universo del discurso no se limita a la producción de informes contables.	En la contabilización de los activos de información se identifican informes internos y externos.
5. Las personas humanas y las organizaciones de personas humanas necesitan que la Contabilidad les provea de resultados que midan cumplimento de objetivos y no solamente ganancias ya que no actúan exclusivamente para obtener ganancias.	En la contabilización de los activos de información se brinda información sobre el cumplimiento de los objetivos planteados.
6. Para resolver todos los problemas que la Contabilidad tiene a su cargo no bastan con los aportes de la Economía.	En la contabilización de los activos de información se encuentran relaciones con otras disciplinas como la tecnología y seguridad de la información.

7. Los sistemas contables particulares, que producen Estados Contables son solamente una parte del dominio o universo del discurso contable.	La contabilización de los activos de información no contradice la ley propuesta de la TGC.
8. En la Contabilidad cohabitan muchos otros elementos de los cuales las prácticas contables, generalmente aceptadas o no, no son principios sino realidades que integran aquel contenido.	En la contabilización de los activos de información se identificaron estándares y buenas prácticas que no son consideradas prácticas contables generalmente aceptadas.
9. Dentro del dominio o universo del discurso contable, las tareas de control económico constituyen una pequeña parte.	En la contabilización de los activos de información se identifican tareas con control relacionadas a cada uno de los niveles de activos identificados.
10. La Contabilidad se ocupa de temas que proveen diversas disciplinas pero por ello no depende de sus respectivas teorías sustentadoras.	La contabilización de los activos de información no depende de las teorías sustentadoras de la tecnología y seguridad de la información.

11. La Contabilidad estudia todos los fenómenos que ocurren en las organizaciones con la intención de ir brindando información sobre cumplimento de metas organizacionales no exclusivamente económicos y no exclusivamente en forma cuantitativa.	La contabilización de los activos de información brinda información organizacional que no se encuentra relacionada con metas económicas y no únicamente en forma cuantitativa.
12. La Contabilidad no está vinculada exclusivamente al principio de dualidad: hay acciones humanas en las organizaciones que no corresponden a ese principio y son materia de la disciplina.	La contabilización de los activos de información no contradice la ley propuesta, ya no se encuentra vinculada con el principio de la dualidad.
13. La Contabilidad tiene un campo amplio de actuación que no se limita a considerar exclusivamente a las transacciones.	La contabilización de los activos de información no se dedica a la registración de transacciones.

14. Aunque la Contabilidad tiene relación con la Teoría de la Medición, es independiente de ella en muchos aspectos de su actuación.	La contabilización de los activos de información no contradice la ley propuesta para la TGC.
15. No es posible expresar las relaciones y mediciones contables exclusivamente en términos monetarios.	La contabilización de los activos de información no se realiza en términos monetarios.
16. El dominio o universo del discurso contable abarca hechos y actos del pasado, del presente y del futuro.	El dominio del discurso contable de los activos de información abarca la registración de hechos del pasado, del presente y la posibilidad de inferirlos en el futuro.

Capítulo VI

6. Segmentación de la contabilización de los activos de información

6.1. Segmentos contables identificados

El cuarto problema identificado es el relacionado con la segmentación contable, los citados autores, plantearon la siguiente hipótesis: "*La Contabilidad tiene una parte general y luego segmentos diversos*." (Elementos para una teoría general de la contabilidad, 2001).

Si bien, como indica el autor Walter Chiquiar (2018):

> *"La Contabilidad Financiera ha primado históricamente sobre los otros segmentos contables, por lo que existe una creencia generalizada de que todo aquello que no se pueda medir en dinero no es parte de la Contabilidad."*

Sobre estas definiciones y amplitud conceptual se encarará la presente investigación en donde se identifican los siguientes segmentos contables:

ESQUEMA N°17: Segmentos Contables

Fuente: Elaboración propia.

Existen otros segmentos identificados a lo largo de la historia contable, donde existe una interpretación de la contabilidad monetaria y la identificada como contabilidad no monetaria. Desde esta concepción, la contabilización de activos de información se encuadra en el segmento contable no monetario.

El autor Mattessich (2002, pág. 8) argumenta que: "*La necesidad de una presentación generalizadora de la Contabilidad se manifiesta de diversas maneras; una de ellas es la aparición de un gran número de sistemas contables en la práctica concreta (…) Estos sistemas contables cumplen diferentes funciones y aún así, están basados en los mismos principios básicos (…)*", planteando que todos los sistemas de información, ya sean microsociales o macrosociales, pueden cumplir diferentes objetivos pero están enmarcados en la Teoría General Contable.

Por lo expuesto precedentemente, el autor de la presente tesis considerará que la contabilización de la información en entidades bancarias pertenece al segmento no monetario con características propias de la contabilidad de gestión. Con el objetivo de identificar las bases teóricas para describir los elementos necesarios para establecer un marco teórico para este modelo contable, se identificarán las bases del Marco General Contable.

6.2. Análisis de las leyes propuestas para la segmentación contable

A continuación, se analizarán las leyes propuestas por los autores para la relación segmentación contable:

ESQUEMA N°18: Contrastación sobre la segmentación contable

Leyes sobre la segmentación contable enunciadas por los autores CLGC, LFG y MCRDM.	Contrastación de las leyes en el contexto de la contabilización de activos de información.
1. La Contabilidad cuenta con una Teoría General Contable aplicable a todas las situaciones pero a ella se agregan modelos, hipótesis y leyes específicas para cada uno de sus segmentos.	La contabilización de los activos de información no contradice la ley propuesta. Representa un modelo no monetario con características en la identificación de los activos de información.
2. La Contabilidad Patrimonial o Financiera está orientada a los individuos ajenos al ente, principalmente, inversores de riesgo (accionistas - acreedores).	La contabilización de los activos de información no contradice la ley propuesta de la TGC.

3. La Contabilidad Gerencial se orienta a servir los intereses de los decididores internos de las organizaciones.	La contabilización de los activos de información proporciona información para los decididores internos de las organizaciones.
4. La Contabilidad Social procura medir en términos diferentes a lo que sugiere la Economía pues las metas sociales, tanto macro como micro, exceden el reduccionismo economicista.	La contabilización de los activos de información no contradice la ley propuesta para la TGC.
5. La Contabilidad Económica o Nacional tiene objetivos derivados de Teorías Económicas y por ende sus modelos se diferencian de los propios de la Contabilidad Patrimonial.	La contabilización de los activos de información no contradice la ley propuesta para la TGC.
6. La Contabilidad Gubernamental tiene como destinatario no sólo a los funcionarios públicos sino a la ciudadanía en general.	La contabilización de los activos de información no contradice la ley propuesta para la TGC.

7. La Contabilidad abarca a la Macrocontabilidad y a la Microcontabilidad con modelos particulares para cada una de ellas.	La contabilización de los activos de información en entidades financieras forma parte de la microcontabilidad, pero también puede identificarse una macrocontabilidad de los activos de información por parte del estado.
8. La Contabilidad tiene dos partes reconocidos como Monetario y No Monetario y cada uno de ellos se puede desarrollar eficazmente sin ignorar los principios comunes de la Teoría General Contable.	La contabilización de los activos de información en entidades financieras forma parte del segmento no monetario.
9. Cada segmento contable tiene un elemento particular que lo hace diferente a los demás.	La contabilización de los activos de información no contradice la ley propuesta de la TGC.

Capítulo VII

7. Identificación del sistema contable de activos de información

7.1. Introducción

Para el quinto problema relacionado a los Sistemas Contables, citados los autores plantean la hipótesis de que: *"Los sistemas contables son creaciones humanas reales para responder a demandas circunstanciales en base a la teoría general contable.*" (García Casella, Fronti de García, & Rodríguez de Ramírez, Elementos para una teoría general de la contabilidad, 2001). Partiendo desde esta concepción y tomando como base la definición de sistema contable publicada por la Comisión Nacional de Valores (2020), en donde lo describe como un *"conjunto de elementos interrelacionados, destinados al registro de las operaciones y hechos económicos-financieros… (…) el mismo comprende los elementos de organización, control,*

guarda o conservación, exposición y análisis…" y considerando que el Marco General de Teoría Contable establece que para cada modelo contable existe un sistema o subsistema de información que tiene el objetivo de recolectar datos, sistematizarlos y brindar información para la toma de decisiones; en el presente capítulo se describe el sistema contable existente en la gestión de activos de información.

En el contexto específico de las entidades bancarias, se puede identificar un sistema de información que registra y documenta los activos de información. Dentro de las funciones propias, se pueden destacar los siguientes objetivos:

- Identificar los activos de información existentes en la entidad.
- Establecer y actualizar un inventario de activos de información.
- Establecer la clasificación de los activos en base a su criticidad y sensibilidad.
- Recolección de logs o pistas de auditoría de seguridad de los activos.
- Brindar reportes de sistemas sobre alta, baja y modificación de los permisos de accesos, puestos, roles y función del personal a cargo.
- Recolectar información sobre los incidentes de seguridad.
- Establecer indicadores de gestión de los activos de información.
- Brindar información calificada para otros sistemas de gestión (Seguridad de la información, Riesgos, Calidad y Continuidad del negocio).

7.2. El sistema de activos de información contable

El “sistema contable de activos de información” o “sistema de activos de información contable" (SAIC) en las entidades bancarias brinda principalmente información relevante a los siguientes sistemas de gestión:

- ✓ Sistema de gestión de seguridad de la información
- ✓ Sistema de gestión de la calidad
- ✓ Sistema de gestión de riesgos
- ✓ Sistema de gestión de continuidad del negocio

Si bien para el caso de entidades bancarias en la República Argentina, el BCRA dispuso en la Comunicación “A” 4609 que las entidades deben tener un registro de los activos de información, este tiene un alcance superior al establecimiento del inventario de activos de información dado que la norma establece “*con el objeto de reducir a un nivel aceptable los riesgos internos y externos de accesos no autorizados, pérdidas y daños a la información*” [xi] , se deben implementar adecuadamente:

- ➢ Registros operativos de las actividades de los usuarios
- ➢ Registros de las tareas realizadas
- ➢ Registros de las funciones utilizadas
- ➢ Reportes de seguridad que registren la asignación de claves y derechos de accesos empleo de programas de utilidad que permitan el manejo de datos por fuera de las aplicaciones
- ➢ Reportes de seguridad de actividades de los usuarios privilegiados
- ➢ Reportes de seguridad de usuarios de emergencia y con accesos especiales

- Reportes de seguridad de intentos fallidos de acceso
- Reportes de seguridad de bloqueos de cuentas de usuario
- Reportes de auditoría que registren las excepciones y actividades críticas de las distintas plataformas.

Además, las entidades deben implementar Tableros de Comando sobre la gestión de estos activos de información, como también monitoreos y alertas. En el punto 3.1.4.5. “Alertas de seguridad y software de análisis” de la Comunicación “A” 4609, se establece que:

> *“deben implementar funciones de alertas de seguridad y sistemas de detección y reporte de accesos sospechosos a los activos de información, (…), y contar con monitoreo constante de los accesos a recursos y eventos críticos, que reporten a los administradores sobre un probable incidente o anomalía en los sistemas de información (…)”*

Para poder dar respuesta a estos requerimientos, el SAIC debe contener un inventario de activos de información definido y actualizado. Para ello, se recomiendan utilizar herramientas o implementar sistemas con la funcionalidad de detectar los activos existentes en la infraestructura de hardware y software como el Sistema de Administración de Configuración de Bases de Datos (Configuration Management Database: CMDB) y el Sistema de Gestión de Información y Eventos de Seguridad (Security Information and Event Management: SIEM) que tiene como objetivo recolectar, almacenar, interpretar y correlacionar logs o pistas de auditoría de seguridad, permitiendo establecer alertas de seguridad o análisis forense de la

información. Asimismo, se pueden integrar los sistemas para evitar fuga de información (Data Loss Prevention: DLP).

En el siguiente esquema se puede identificar los elementos básicos del “SAIC” en entidades bancarias:

ESQUEMA N°19: Elementos básicos del sistema de activos de información contable elementos (SAIC).

Fuente: Elaboración propia.

7.3. El inventario de activos de información en entidades bancarias

En la sección V de la Comunicación “A” 4609 del BCRA, se establece que las entidades bancarias deben implementar un sistema de gestión de activos de información:

> *“Las entidades financieras deben contar con la capacidad de identificar sus activos informáticos y de información, las características, la localización y la criticidad e importancia de los mismos.”*

En este caso, el organismo de control instruye que las entidades deben establecer un inventario de activos de información, considerando las categorías indicadas en el capítulo anterior. Asimismo, indica que deben contar con procedimientos para identificar sus activos que pueden ser por procesos manuales o sistemas que monitorean y detectan activos de información.

> *“Sobre la base de esta información, las entidades financieras podrán asignar niveles de protección proporcionales a la importancia de los activos, realizar una continua categorización de los mismos, mantenerlos actualizados y efectuar el mantenimiento preventivo de sus recursos físicos.”* (BCRA, 2006).

En este caso, el organismo plantea que las entidades asignen niveles de importancia, categorizándolos, clasificándolos y actualizándolos.

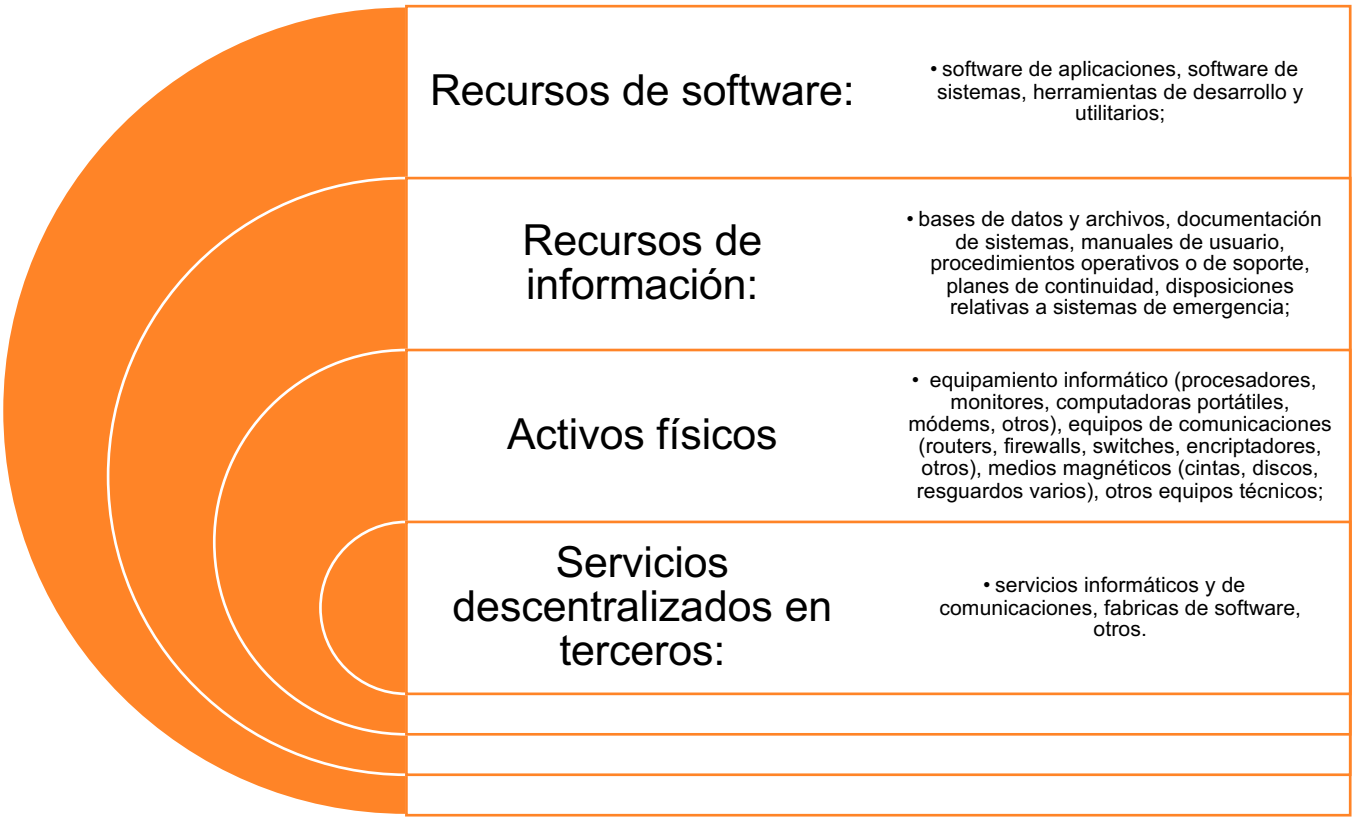
> *“Por ello, las entidades financieras deben elaborar y mantener un inventario de los activos asociados a cada sistema de información. Se debe identificar*

claramente cada activo, estableciendo su propietario y su clasificación en cuanto a seguridad." (BCRA, 2006).

En este párrafo, el organismo establece la creación de un inventario de "activos de información" con la relación de estos elementos. Asimismo, incluye la necesidad de asignar un propietario y su clasificación en relación con los principios de la seguridad de la información.

Un óptimo inventario de activos de información debería contener el detalle de todos los componentes existentes (N1, N2, hasta la categoría N8) y su relación. En esta línea el BCRA establece contener como mínimo los siguientes elementos:

ESQUEMA N°20: Estructura de elementos básicos del inventario de activos.



Fuente: (BCRA, 2006)

En esta reglamentación se especifican las características mínimas que debe tener el inventario de activos. Como también se establece el procedimiento mínimo de clasificación de la información contenida en cada uno de los activos de información identificados, como por ejemplo:

ESQUEMA N°21: Requerimientos al Sistema Contable de Activos de Información.

Requerimientos del BCRA al sistema contable de activos de información	Consideraciones
"Las entidades financieras deben clasificar sus activos de información de acuerdo con su criticidad y sensibilidad, estableciendo adecuados derechos de acceso a los datos administrados en sus sistemas de información."	En el sistema de información se deben identificar y sistematizar los activos de información existentes, además de analizar su criticidad y una adecuada administración de los derechos de acceso.
"Esta clasificación deberá ser documentada, formalizada y comunicada a todas las áreas de la entidad, principalmente a los propietarios de los datos. La misma puede ser parte integrante de la política de protección de los activos de	En el sistema de información debe ser capaz de poder clasificar la información y asignar responsables de la misma (lo que en la norma se denomina responsables).

información, o formar un documento aparte."	Se debe documentar todos los procedimientos de esta sistematización.
"Los niveles de acceso deben diseñarse considerando los criterios de la clasificación, junto con una adecuada separación de tareas, determinando qué clases de usuarios o grupos poseen derechos de acceso -y con qué privilegio- sobre los datos, sistemas, funciones y servicios informáticos. La asignación de derechos de acceso debe otorgarse a través de un proceso de autorización formal del propietario de los datos, verificando periódicamente los niveles y privilegios otorgados a los usuarios."	El sistema de información debe brindar la información necesaria para poder asignar una correcta alta, baja o modificación de accesos de usuarios y perfiles a programas y sistemas.
Fuente: (BCRA, 2006)	

En este sentido, se destaca que la información de gestión del inventario de los activos de información debe:

> "*permitir identificar el tipo de información que contienen, han de ser inventariados y además almacenados en lugares con acceso restringido sólo al personal autorizado. Los soportes que tengan datos protegidos, sea como consecuencia de operaciones temporales de la propia aplicación que los trata, o como consecuencia de procesos periódicos de apoyo o cualquier otra operación espontánea, deberán estar claramente identificados con una etiqueta externa que indique de qué datos se trata."* (López, Moya, Marimón, & Planas, 2011)

A continuación, se identifican los controles más relevantes relacionados con la gestión del inventario de activos.

7.4. Estándares internacionales en el manejo de activos de información

En la serie ISO/IEC/IRAM 27.000, se encuentra publicada la 27.002 que establece los lineamientos de control para la implementación de los Sistemas de Gestión de la Seguridad de la Información (SGSI).

En torno al inventario de activos, la misma establece los siguientes controles que deben garantizarse en la gestión de activos:

ESQUEMA N°22: Controles en el SAIC dispuesto por la ISO/IEC/IRAM 27.002

Inventario de activos:

- Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.

Propiedad de los activos:

- Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.

Uso aceptable de los activos:

- Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.

Devolución de activos:

- Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo."

Fuente: (International Organization for Standardization / International Electrotechnical Commission, 2013)

Asimismo, se recomienda que "*todos los activos debieran ser inventariados y contar con un propietario nombrado*" asignando la responsabilidad en los controles correspondientes. (International Organization for Standardization / International Electrotechnical Commission, 2013)

En esta línea, los autores españoles Emilio del Peso Navarro, Miguel Ángel Ramos, Mar del Peso, desarrollaron un "El documento de Seguridad (Análisis Técnico y Jurídico. Modelo)" en donde establecieron elementos básicos en la administración de los datos:

"Modelo de seguridad protegidos:

Inventario de Hardware

Inventario de software

Inventario de ficheros y bases de datos

Configuración del sistema informático

Organigrama de la empresa

Prestación de servicios

Estructura de los ficheros y bases de datos

Descripción del sistema de información

La información requerida puede afectar a:

Centro de datos

Servidores

Ordenadores personales

Ordenadores portátiles

Estaciones de trabajo

Otros terminales

Internet e intranet." (Peso Navarro, Ramos, & Peso, 2004)

7.5. Información brindada por el SAIC

Como se indicó precedentemente, el sistema contable de activos de información para satisfacer las necesidades de las entidades bancarias debe contener mínimamente los siguientes conceptos:

- Indicadores de seguridad de la información (Tablero de comando).
- Información suministrada de los eventos de sistema de gestión de información y eventos de seguridad (SIEM).
- Información suministrada por el sistema de administración de gestión de bases de datos (CMDB).
- Información suministrada por el sistema de prevención de fuga de información (DLP).
- Reportes de la gestión del inventario y clasificación de activos.
- Reportes sobre la gestión de incidentes se seguridad.

Como se puede observar, se destacan diversos indicadores de los activos de información, y los mismos pueden ser agrupados por tipo de dato. Se destaca la visión de Fabián Portantier, en donde indica que deben desarrollarse 2 tipos de métricas:

> *"La primera debe tener un enfoque técnico y nos servirá para analizar en qué puntos tenemos que mejorar, qué vulnerabilidades debemos atacar primero, qué medidas de seguridad están teniendo éxito, etc."*

> *"El segundo reporte debe ser dirigido a la dirección de la empresa y su objetivo es mostrar aspectos genéricos de la seguridad (…), por ejemplo, qué se debe mejorar, incluir propuestas de inversión, ya sean recursos tecnológicos, recursos humanos o capacitaciones al personal".* (Portantier F. , 2013)

A los interesados en identificar las métricas básicas que deberían considerarse en el tablero de comando del SAIC, en el capítulo X de la presente tesis se analizarán los indicadores a nivel estratégico, táctico y operativo existentes en las entidades bancarias.

7.6. Conclusiones particulares del capítulo VII

El sistema contable de activos de información (SAIC) en las entidades bancarias brinda principalmente información relevante a los siguientes sistemas de gestión: seguridad de la información, calidad, gestión de riesgos y continuidad del negocio, entre otros.

Si bien, para el caso de entidades bancarias en la República Argentina, el BCRA dispuso en la Comunicación "A" 4609 que las entidades deben tener un registro de los activos de información, el mismo tiene un alcance superior al establecimiento del inventario de activos de información, dado que se deben implementar adecuadamente:

- Registros operativos de las actividades de los usuarios
- Registros de las tareas realizadas
- Registros de las funciones utilizadas

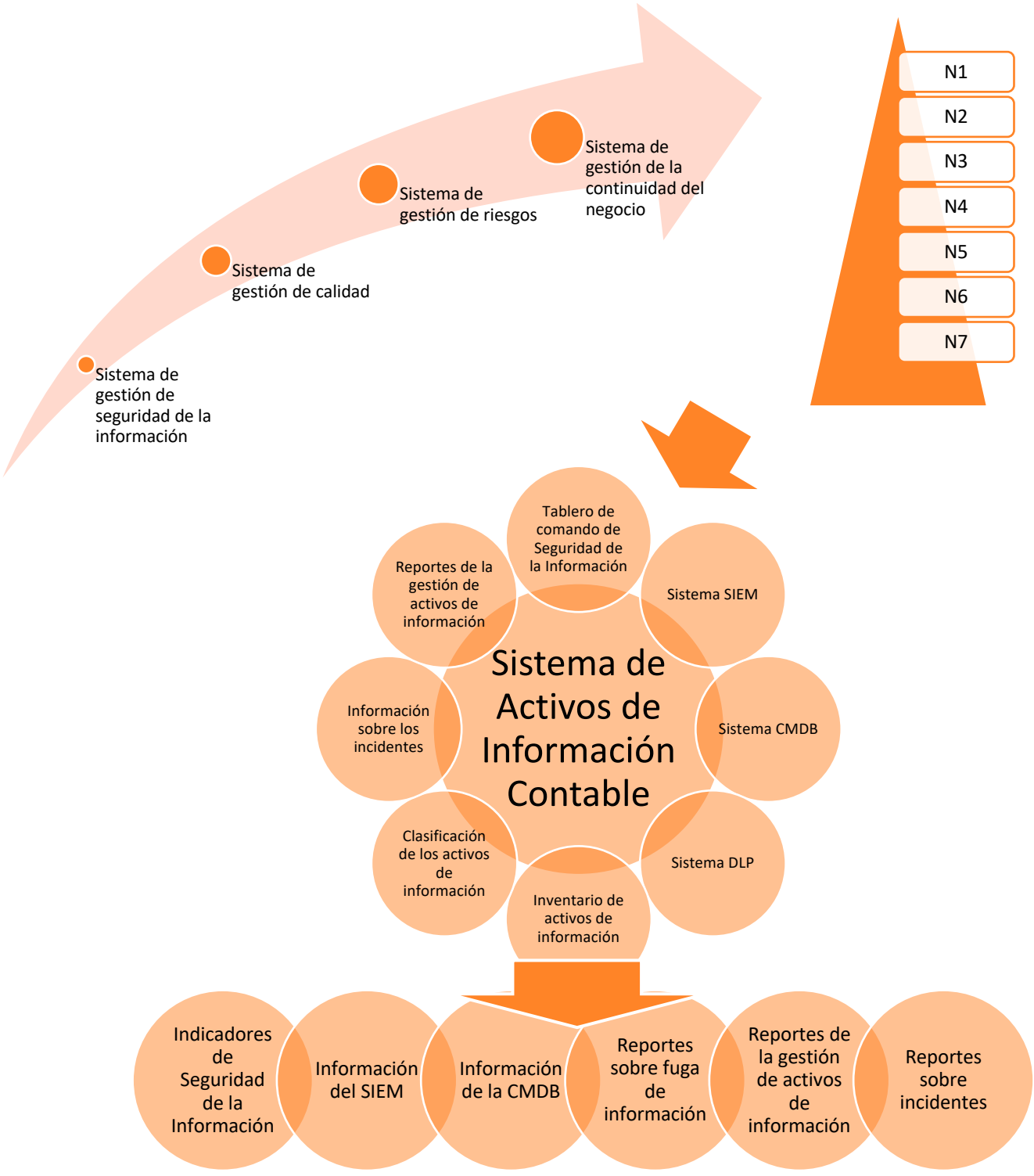
- Reportes de seguridad que registren la asignación de claves y derechos de accesos empleo de programas de utilidad que permitan el manejo de datos por fuera de las aplicaciones
- Reportes de seguridad de actividades de los usuarios privilegiados
- Reportes de seguridad de usuarios de emergencia y con accesos especiales
- Reportes de seguridad de intentos fallidos de acceso
- Reportes de seguridad de bloqueos de cuentas de usuario
- Reportes de auditoría que registren las excepciones y actividades críticas de las distintas plataformas.

Bajo estos requisitos, el sistema de activos de información contable (SAIC) en las entidades bancarias está compuesto mínimamente por los siguientes componentes:

- Tablero de comando / indicadores de seguridad de la información
- Sistema de gestión de información y eventos de seguridad (SIEM)
- Sistema de administración de gestión de bases de datos (CMDB)
- Sistemas de prevención de fuga de información (DLP)
- Inventario de activos de información
- Clasificación de los activos de información
- Información sobre los incidentes de seguridad de la información
- Reportes de la gestión de activos de información

El cual brinda información para una eficiente gestión de los activos de información. En el siguiente esquema se puede identificar las relaciones del SAIC con los sistemas de gestión.

ESQUEMA N°23: Relaciones del SAIC y los sistemas de gestión



Fuente: Elaboración propia.

Para contrastar el sistema contable no monetario de activos de información, en el siguiente cuadro se analizan las leyes planteadas para los sistemas contables:

ESQUEMA N°24: Contrastación sobre los sistemas contables

Leyes sobre los sistemas contables enunciados por los autores CLGC, LFG y MCRDM.	Contrastación de las leyes en el contexto de la contabilización de activos de información.
1. La Contabilidad propone la creación de sistemas contables frente a necesidades particulares, pero siempre basándose en la Teoría General Contable.	En la contabilización de los activos de información se identifica un sistema contable único con características propias al cumplimiento de los objetivos.
2. Los sistemas contables abarcan todo lo que habitualmente se llama sistema de información de un ente si se basan en una Teoría General Contable que exceda los límites de la Contabilidad Patrimonial o Financiera.	En el sistema de activos de información contable (SAIC) se reconocen eventos y hechos que no están relacionados con la contabilidad patrimonial.
3. Hay Sistemas Contables Macro que abarcan la normativa o las	En la contabilización de activos de información se identifican

reglas de un lugar geográfico determinado y Sistemas Contables Micro propios de un ente y dedicado a diseñar sus componentes materiales y humanos.	macrosistemas contables que abarcan lugares geográficos como la Ciudad Autónoma de Buenos Aires, o en el ámbito de la AAIP en relación con las bases de datos registradas a nivel nacional.
4. Los sistemas contables micro, propios de cada organización, se alimentan de las propuestas de la Teoría General Contable.	En los sistemas de activos de información contable microsociales (SAIC), las entidades toman en cuenta las propuestas de la TGC.
5. La Contabilidad utiliza las herramientas que proporciona el procesamiento electrónico de datos para diseñar los sistemas contables micro.	En la contabilización de activos de información se utilizan herramientas y sistemas tecnológicos para agilizar procesamientos y diseñar un SAIC acorde a las necesidades de la entidad.
6. Los diseñadores de los sistemas contables de cada organización deciden cual puede ser el mejor método de registración sin limitarse exclusivamente al llamado de partida doble.	En la contabilización de activos de información no se utiliza la técnica de la partida doble.

7. Los sistemas contables actuales se estructuran cada vez más en bancos de datos que recogen información útil y la ofrecen a los distintos usuarios.	En la contabilización de activos de información se utilizan modelos automatizados para diseñar un SAIC acorde a las necesidades de la entidad.
8. El sistema contable que se ocupa de todos los datos transformables en información, de un ente determinado, abarca hechos, actos y objetos de muy diversa índole.	En el sistema de activos de información contable (SAIC) se identifican todos datos relacionados a diversos sistemas y los transforma en información para la toma de decisiones.
9. Aunque los componentes de los sistemas contables deriven de Modelos y Segmentos Contables diversos es posible reunirlos en una única base de datos con un diseño especial para estos sistemas contables amplios.	La contabilización de los activos de información no contradice la ley propuesta de la TGC.
10. La Contabilidad, que tiene un dominio o universo del discurso contable amplio, no se reduce a aplicaciones del principio de	La conceptualización de la contabilización de activos de

dualidad en los sistemas que genera.	información se basa en el discurso contable amplio.
11. Todo sistema contable se debe diseñar contemplando las necesidades de los usuarios de la información contable que va a emitir.	Los sistemas de activos de información contable (SAIC) se diseñan teniendo en cuenta las necesidades de los usuarios de información.
12. Los sistemas contables deben aprovechar al máximo las entradas seleccionadas para ofrecer las mejores salidas para diversas necesidades.	En los sistemas de activos de información contable (SAIC) se aplican correcciones para mejorar la emisión de información.
13. Todo sistema contable de una organización debe tener, como mínimo: registros contables, métodos de registración, medios de registración, plan de cuentas, manual de cuentas, archivos de comprobantes, control interno o seguridad y nómina de informes a emitir.	En los sistemas de activos de información contable microsociales (SAIC) se identifican: Registros contables no monetarios, métodos de registración, nómina de activos de información, manual de clasificación de activos, control interno, logs de seguridad y lista de informes a emitir.

Capítulo VIII

8. Modelos teóricos para la medición de los activos de información

8.1. Introducción

En todo modelo contable se deberían establecer métodos de medición para los elementos analizados. Alejandro Agustín Barbei en su tesis doctoral afirma que: "*La disciplina contable utiliza distintas escalas de medición y esto determina las operaciones que pueden realizarse con estas mediciones. Es decir, no todas las mediciones son iguales*." (2017) Asimismo, "*los elementos contables pueden ser descriptos tanto de manera cuantitativa como cualitativa, teniendo en cuenta sus particularidades y los objetivos del usuario.*"

Para el sexto problema planteado por los citados autores relacionados con la medición, plantean que la *"Contabilidad se ocupa de la medición en sentido amplio, tanto cuantitativo como cualitativo y para así poder ofrecer informes que contemplen las preferencias de los participantes de la actividad contable."* (García Casella, Fronti de García, & Rodríguez de Ramírez, Elementos para una teoría general de la contabilidad, 2001)

En el caso particular de los activos de información identificados en las entidades bancarias, existen métodos utilizados para su medición. Los mismos están basados en ponderaciones cualitativas no monetarias. Para interpretarlos primero se debe definir el término de "amenaza" que pueden tener los activos, en donde se puede ver comprometido alguno de los principios de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad (C-I-D).

En esta línea, resulta indispensable reconocer los riesgos a los que se encuentran expuestos nuestros activos de información. El autor Arboledas Brihuega expone que:

> *"Los ataques informáticos son aquellos métodos por los cuales se intenta desestabilizar, dañar o tomar el control de un sistema informático ajeno."*
>
> *Se pueden identificar:*
>
> *Interrupción: Este ataque vulnera la disponibilidad de un recurso informático.*
>
> *Intercepción: Este ataque vulnera la confidencialidad, pues un intruso ha accedido a información para la que no está autorizado.*

Fabricación: Se vulnera la autenticidad, pues se trata de modificar la información para que sea similar al recurso original.

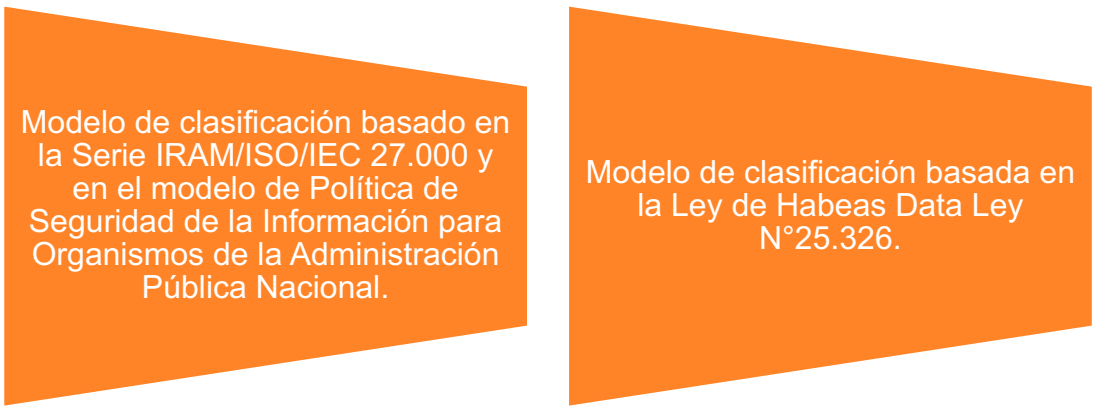
Modificación: Ataca la integridad de los datos, pues se ha cambiado sin la autorización correspondiente en algún momento entre su creación y la recepción por parte del destinatario." (2014)

En base a esta enumeración de ataques, se desarrollan los modelos de medición de los activos de información los cuales toman como base a la criticidad de los datos.

8.2. Modelización de la medición de activos de información

En el ámbito de la República Argentina pueden identificarse dos modelos para el análisis de la información existente en entidades bancarias:

ESQUEMA N°25: Modelización de la criticidad de la información



Fuente: Elaboración propia.

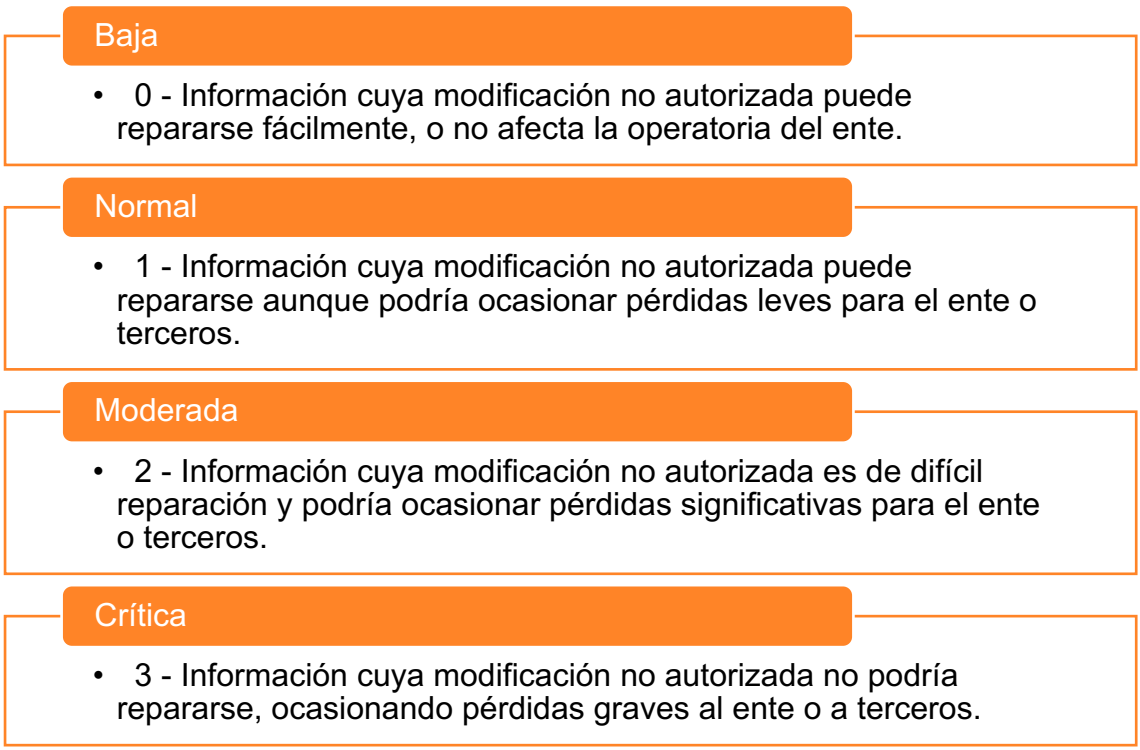
8.3. Modelo de clasificación basado en la serie IRAM/ISO/IEC 27.000

El Modelo de clasificación basado en la serie IRAM/ISO/IEC 27.000 y en el modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional (ONTI, 2020), adaptado a todo tipo de entes, establece que los activos de información deben clasificarse de acuerdo con los principios básicos de la Seguridad de la Información: Confidencialidad, Integridad y Disponibilidad, siempre y cuando la dimensión aplique al nivel de activo analizado.

8.3.1. Niveles de clasificación según la Integridad de la Información:

Se establecen 4 niveles para clasificar la información existe en relación con la integridad:

ESQUEMA N°26: Clasificación según la Integridad



Fuente: Elaboración propia basado en el Modelo publicado por la (ONTI, 2020).

8.3.2. Niveles de clasificación según la Confidencialidad de la Información:

Se establecen 4 niveles para clasificar la información existente en relación con la confidencialidad:

ESQUEMA N°27: Clasificación según la Confidencialidad

Información Pública

- 0 - Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado del ente o no.

Información Reservada o de uso interno

- 1 - Información que puede ser conocida y utilizada por todos los empleados del ente y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el ente, el Sector Público Nacional o terceros.

Información Reservada o Confidencial

- 2 - Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al ente o a terceros.

Información Secreta

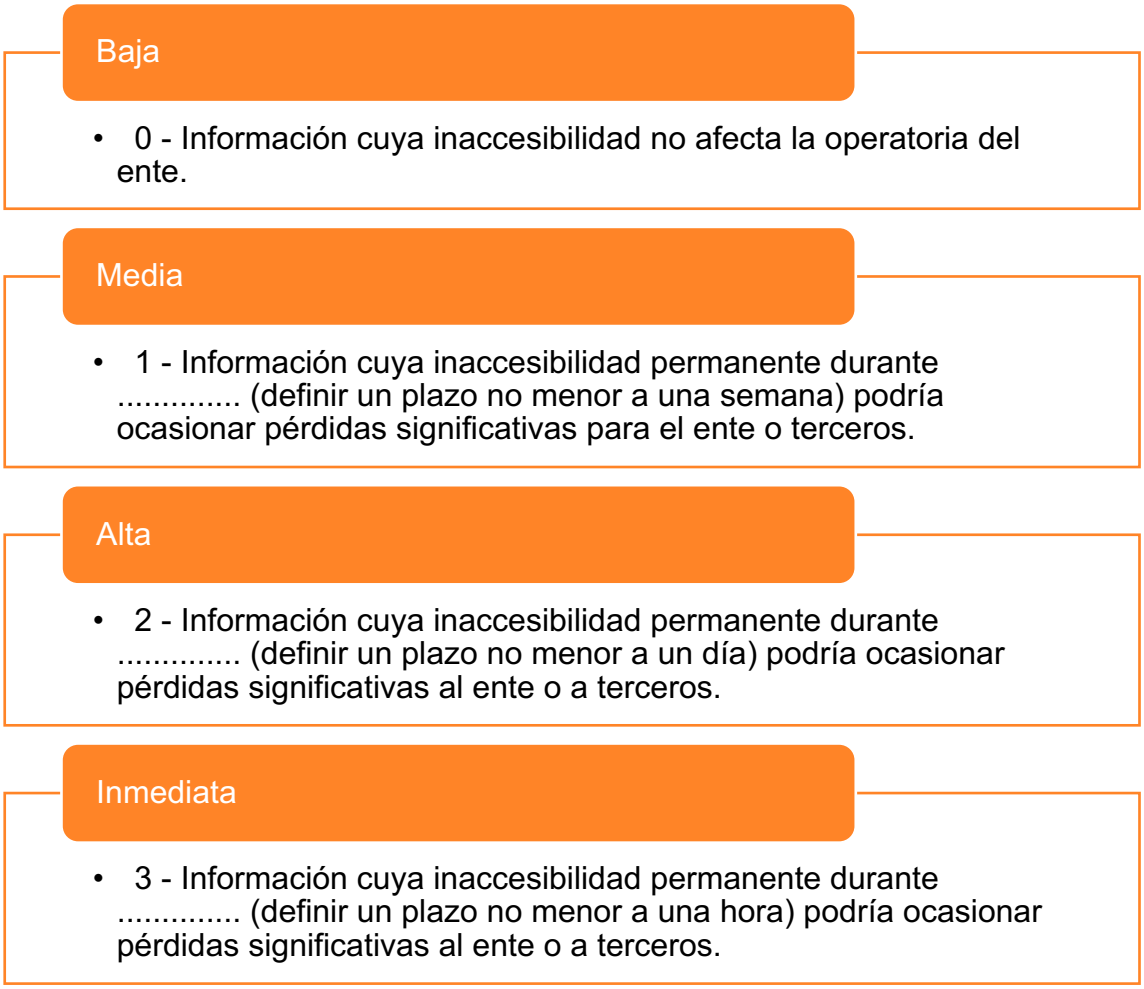
- 3 - Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del ente, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo o a terceros.

Fuente: Elaboración propia basado en el Modelo publicado por la ONTI (ONTI, 2020).

8.3.3. Niveles de clasificación según la Disponibilidad de la Información:

También se establecen 4 niveles para clasificar la información existente en relación con la disponibilidad:

ESQUEMA N°28: Clasificación según la Disponibilidad

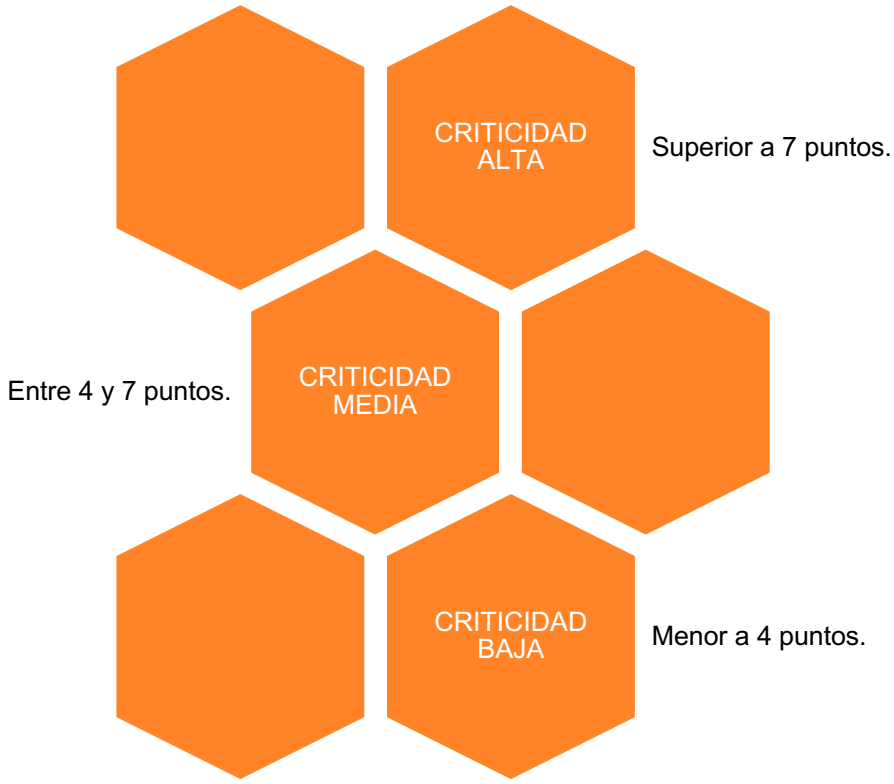


Fuente: Elaboración propia basado en el Modelo publicado por la (ONTI, 2020).

En base a "*este análisis de cada uno de los activos de información, debemos realizar la suma algebraica de los tres términos analizados*" (Escobar, 2017).

Siguiendo esta metodología, se deben establecer los umbrales para definir la criticidad. En modo de ejemplo se presenta el siguiente esquema de criticidad:

ESQUEMA N°29: Criticidad de la información



Fuente: Elaboración propia.

En donde nos arrojaría como resultado el posicionamiento de la información ordenada desde la más crítica a la menos crítica, acorde a la clasificación de la misma.

8.4. Clasificación dispuesta por la Ley N°25.326

El principal objetivo de la ley de referencia es la:

> "*protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.*" (Escobar, Ley de Protección de Datos Personales, 2010).

La citada normativa y las Disposiciones de la Agencia de Acceso a la Información Pública (AAIP) ex-Dirección Nacional de Protección de Datos Personales, "*han establecido una clasificación a los mismos, en Datos Básicos, Intermedios y Sensibles*". (Suarez Kimura & Escobar, Repercusiones de La Ley De Protección de Datos Personales en el Ejercicio Profesional del Contador Público, 2010).

ESQUEMA N°30: Clasificación de Datos Personales

Fuente: Elaboración propia.

Los datos considerados básicos, corresponden a los existentes en el padrón electoral. Entre ellos encontramos al número de Identidad, Nombre y Apellido, CUIT, CUIL, Domicilio, Fecha de Nacimiento, entre otros.

Los datos intermedios son los que superan a los básicos y no son sensibles. Por ejemplo, estado civil, ingresos y egresos, etc.

Los datos sensibles son datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Considerando la presente normativa, la documentación contable analizada por el Contador Público en las organizaciones (en el caso en que incluyan datos personales), deberá ser clasificada considerando sus datos contenidos, como también se debe cumplir con las medidas de seguridad dispuestas por la AAIP.

Generalmente, la información contenida en los comprobantes y documentación de comercio con la identificación de los clientes o proveedores es considerada intermedia porque con los datos contenidos en los mismos se pueden determinar el ingreso y el consumo de estos, sus gustos y preferencias por productos o marcas, entre otras cosas.

En el caso de las bases de datos con información de sus empleados, están conformados por datos intermedios y sensibles, que son utilizados para confeccionar declaraciones juradas, aportes y contribuciones, asignaciones familiares, entre otros.

8.5. Controles específicos en la clasificación dispuestos en la IRAM/ISO/IEC 27.002:

En el marco de los controles establecidos para clasificación de los activos de información, la IRAM/ISO/IEC 27.002 establece los siguientes puntos de control para esta clasificación:

> *"**Directrices de clasificación:** La información debería clasificarse en relación con su valor, requisitos legales, sensibilidad y criticidad para la Organización (…),*
>
> ***Etiquetado y manipulado de la información:** Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización (…),*
>
> ***Manipulación de activos:** Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización."*

La normativa analizada destaca la importancia de seleccionar un método con todas las características mínimas a ser consideradas. La normativa establece que los activos de información deben estar etiquetados y recibir el adecuado tratamiento, en base a la información analizada. Y por último, establece la necesidad de contar con procedimientos acordes con el esquema de clasificación adoptado.

8.6. Conclusiones particulares del capítulo VIII

Uno de los requisitos más relevantes en el armado de un Modelo Contable particular, radica en la necesidad de establecer criterios de medición acordes al ámbito de aplicación. En este caso, el modelo descripto se encuadra dentro de los modelos no monetarios, lo que plantea la necesidad de valuaciones cualitativas con ponderaciones cuantitativas para su análisis.

Una de las metodologías más utilizadas para clasificar la información surge de la serie IRAM/ISO/IEC 27.000 en donde se analiza la criticidad teniendo en cuenta la disponibilidad, confidencialidad e integridad de los datos, con una ponderación para establecer la criticidad y sensibilidad de los activos de información.

Otra de las formas es la establecida por la ley de Habeas Data y las Disposiciones de la Agencia de Acceso a la Información Pública, en donde clasifica a la información teniendo en cuenta si existen datos personales y si esos mismos contienen datos básicos, intermedios o sensibles.

Considerando que la Comunicación “A” 4609 del BCRA, establece que *“las entidades financieras deben clasificar sus activos de información de acuerdo con su criticidad y sensibilidad”* y que los estándares internacionales asociados al tema establecen que *“la información debería clasificarse en relación con su valor, requisitos legales, sensibilidad y criticidad para la Organización”,* habría que considerar ambas para poder clasificar los activos de información existentes en las entidades bancarias.

A continuación, se analizarán con las leyes de la TGC propuestas para la medición y su contrastación con el modelo contable alternativo para los activos de información:

ESQUEMA N°31: Contrastación sobre los sistemas contables

Leyes sobre la medición enunciados por los autores CLGC, LFG y MCRDM.	Contrastación de las leyes en el contexto de la contabilización de activos de información.
1. La Contabilidad proporciona exteriorizaciones numéricas acerca de propiedades cuantitativas y cualitativas de distintos objetos y de relaciones y fenómenos sociales de seres humanos.	La contabilización de activos de información proporciona exteriorizaciones numéricas sobre los diferentes elementos registrados.
2. La Contabilidad utiliza diversas escalas de medición; algunas de ellas son la nominal, la ordinal, la de intervalos y la de razones.	La contabilización de activos de información proporciona un método de medición de los activos por medio de intervalos considerando la integridad, la confidencialidad y la confidencialidad.

3. La mayoría de las realidades sociales a contabilizar pueden observarse a través del examen de documentación.	La mayoría de los eventos relacionados con la contabilización de los activos de información se pueden analizarse a través de los log o pistas de auditoría.
4. La medición contable resulta sumamente difícil, igual que en otras ciencias sociales, por la incertidumbre que rodea la acción humana.	La contabilización de los activos de información no contradice la ley propuesta de la TGC.
5. Pueden utilizarse muchos parámetros diferentes para efectuar mediciones contables: para ello se deben tomar en cuenta las preferencias de los individuos afectados.	La contabilización de los activos de información no contradice la ley propuesta de la TGC. Cada entidad puede utilizar un modelo de criterios diferente para la medición de la criticidad de la información.
6. Los valores a medir no responden exclusivamente a mercados, ni a negociaciones pues se originan en la axiología,	La medición de activos de información se realiza ponderando entre otros principios la integridad, la confidencialidad y la disponibilidad.

parte de la filosofía (antropología filosófica).	
7. El deseo de comparar representaciones contables genera el problema de la unidad de medida.	La contabilización de los activos de información no contradice la ley propuesta de la TGC.
8. No hay una medida contable exacta de un fenómeno.	La contabilización de los activos de información no contradice la ley propuesta de la TGC.
9. No todos los datos pueden agregarse.	En la registración de los activos de información no se utilizan todos los datos para calcular la criticidad.
10. Debemos tener técnicas de medición para objetivos organizacionales variados no exclusivamente financieros.	En la registración de los activos de información se utilizan mediciones no monetarias.

Capítulo IX

9. Personas y sujetos en la actividad contable de los activos de información

9.1. Introducción

La identificación de las personas, entes, su organización y vinculación existente en un modelo contable, es otro de los requisitos a contrastar respecto del Marco General de la Teoría Contable.

Para el séptimo problema, “personas de la actividad contable”, los autores (García Casella, Fronti de García, & Rodríguez de Ramírez, Elementos para una teoría general de la contabilidad, 2001) plantean que *“Las personas en su carácter de sujetos de la actividad contable, tienen características que debe considerar la Contabilidad.”*

Para poder identificar el contexto, resulta fundamental establecer y definir la relación entre los datos, los individuos y la profesión contable.

En esta línea, el Consejo de Decanos de Facultades de Ciencias Económicas de Universidades Nacionales (CODECE) en su documento base para la acreditación de la carrera de Contador Público ha definido que “el objeto de su profesión es la “información” en todas sus formas, sea la misma generada dentro de las organizaciones, interactuando éstas entre sí o en su vinculación con el contexto” (CODECE, 2019).

Esta enunciación establece, en un primer término que los Profesionales en Ciencias Económicas deben prestar atención sobre las consecuencias del impacto que “*han tenido las tecnologías de información y comunicación en los procesos administrativos, la documentación respaldatoria y en infinidad de elementos en una organización, las que terminan repercutiendo en aspectos formales, normativos y legales en el sistema de información contable*” (Escobar, 2013).

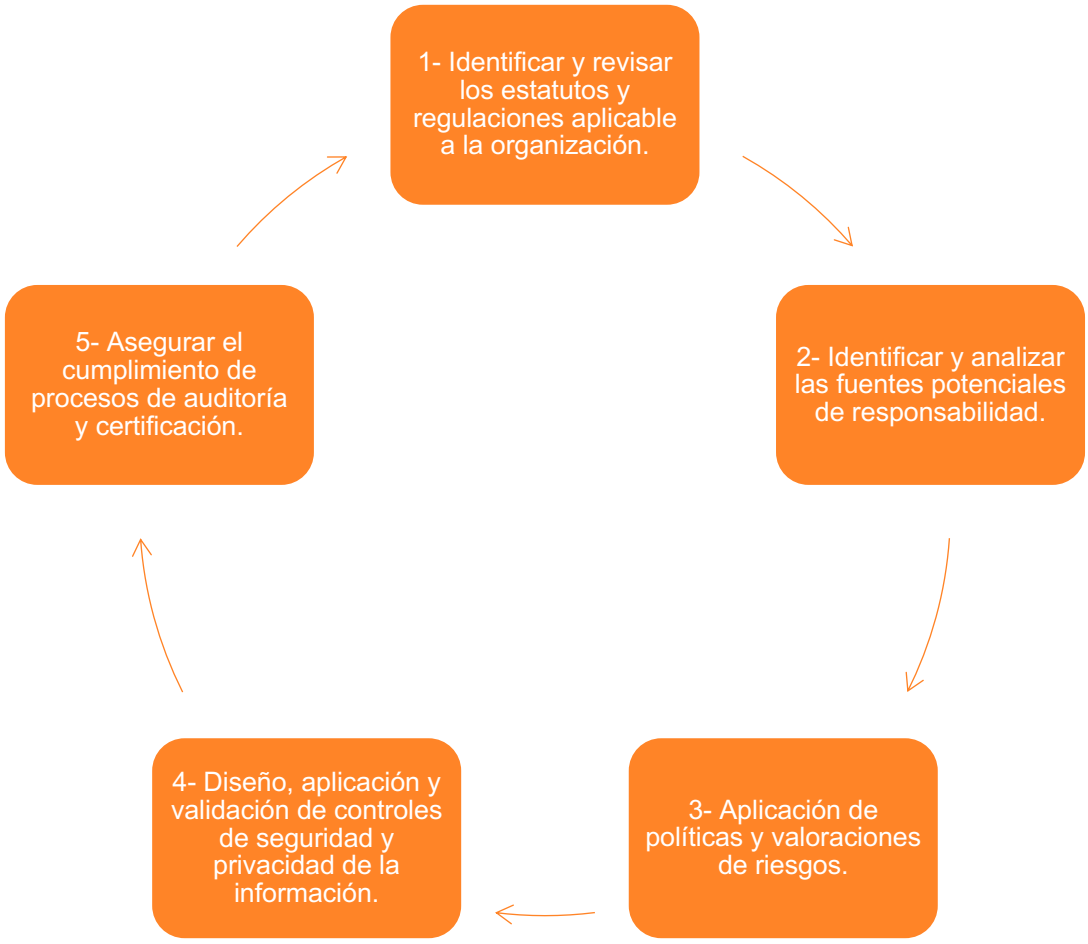
Como se indicó precedentemente, el presente capítulo tiene por objetivo la identificación de los sujetos en la gestión del sistema de activos de información contable y su relación con la Ley de incumbencias profesionales en Ciencias Económicas.

9.2. Ciclo de vida de la información y los roles identificados en su gestión

Para identificar a los actores involucrados resulta imprescindible describir el ciclo de vida de los activos de información. El principal proceso administrativo es el

relacionado con la seguridad; en esta línea el autor Shaw (2011) propone un ciclo de vida para la privacidad y la seguridad de la información:

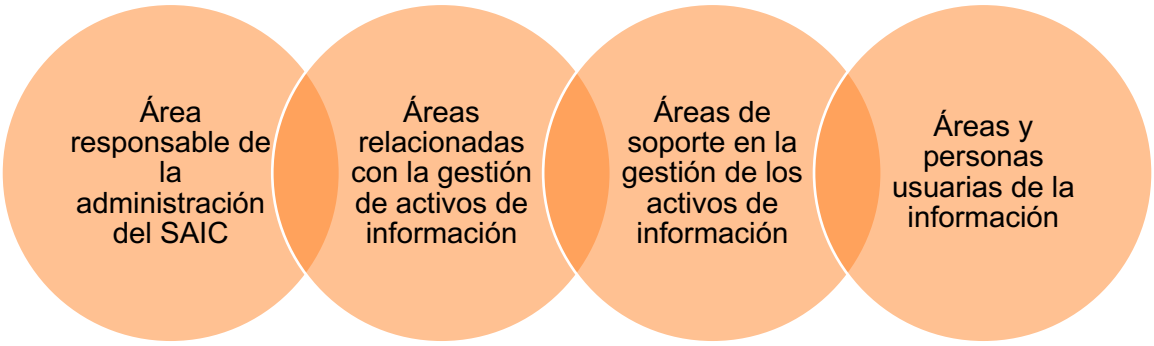
ESQUEMA N°32: Propuesta de ciclo de vida para la privacidad y la seguridad de la información



Fuente: Traducción y e interpretación de (Cano M. J. J., 2013)

En base a este ciclo, en la gestión de los activos de información, se pueden identificar las siguientes áreas involucradas:

ESQUEMA N°33: Áreas relacionadas en la administración del SAIC



Fuente: Elaboración propia.

- Área responsable de la administración del SAIC: El equipo responsable de la planificación, gestión y control del sistema contable de activos de información.
- Áreas relacionadas con la gestión de activos de información: Se destacan las áreas responsables de la gestión de seguridad de la información, calidad, riesgos y continuidad del negocio.
- Áreas de soporte en la gestión de los activos de información: En donde se destacan las áreas de tecnología y sistemas. "*En la actualidad existen muchos profesionales cuyo cargo se denomina: administrador del sistema" (la infraestructura de hardware, software y procedimientos)*." (Cano M. J. J., 2015).
- Áreas y personas usuarias de la información: Conformado por el resto de las áreas y personas de la entidad que tienen conocimiento y utilizan la información para el desarrollo de las actividades.

A continuación, se identificarán las áreas establecidas por el BCRA para la administración de los activos de información.

9.3. Área departamental responsable de la gestión del sistema contable de activos de información

La citada Comunicación "A" 4609, establece como área responsable del manejo del sistema a: "Protección de activos de información" (PAI). La misma norma establece que el mismo "*será responsable de observar la existencia y correcta aplicación de los controles considerados como práctica recomendada y de uso frecuente en la implementación de la protección de los activos de información*" (punto 3.1.5). En el siguiente esquema se identifican los componentes comprendidos:

ESQUEMA N°34: Responsabilidades del área de Protección de Activos de Información dispuesta por el BCRA

En esta línea, el BCRA establece las responsabilidades e incompatibilidades con otras áreas de la entidad que deben ser tenidas en cuenta en el establecimiento de actividades y segregación de funciones.

ESQUEMA N°35: Actividades y segregación de funciones dispuesta por el BCRA

	Análisis funcional / Programación	Control de calidad	Operaciones	Administración de resguardos	Implementaciones	Data Entry	Administración de bases de datos	Administración de redes	Administración de telecomunicaciones	Administración del sistema operativo	Mesa de ayuda	Usuario final	Asignación de perfiles	Definición e implementación de políticas, perfiles y accesos	Control y monitoreo de seguridad informática
Análisis funcional / Programación		X	NO	NO	NO		NO	X	X	NO		NO	NO	NO	NO
Control de calidad	X		NO	NO	X	X	NO	X	X	NO	NO	SI	NO	NO	NO
Operaciones	NO	NO			X	NO	X	X	X	X		NO	NO	NO	NO
Administración de resguardos	NO	NO			X	NO	NO			X	NO	X	NO	NO	NO
Implementaciones	NO	X	X	X		NO	NO			X	X	NO	NO	NO	NO
Data Entry		X	NO	NO	NO		NO	X	X	X	X		NO	NO	NO
Administración de bases de datos	NO	NO	X	NO	NO	NO				X	X	NO	NO	NO	NO
Administración de redes	X	X	X			X						NO	NO	NO	NO
Administrador de comunicaciones	X	X	X			X						NO	NO	NO	NO
Administración de sistemas operativos	NO	NO	X	X	X	X	X					NO	NO	NO	NO
Mesa de ayuda		NO		NO	X	X	X					NO	NO	NO	NO
Usuario final	NO	SI	NO	X	NO		NO	NO	NO	NO	NO			NO	NO
Asignación de perfiles	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO				
Definición e implementación de políticas, perfiles y accesos	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO			
Control y monitoreo de seguridad informática	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO			

Fuente: Comunicación “A” 4609 del BCRA.

Por lo dispuesto, las únicas funciones compatibles con el área de PAI son las siguientes:

- Control y monitoreo de la seguridad informática.
- Definición e implementación de políticas, perfiles y accesos y asignación de perfiles.

Esto hay que considerarlo al planificar los equipos dado que, por sus tareas, el área de PAI es pasible de conflictos con otras áreas, como tecnología, administración de sistemas operativos, bases de datos, etc. En este sentido, el autor (Cano M. J. J., 2015) manifiesta que:

> *"El concepto de seguridad y control no debe estar fundado en la capacidad de restricción, sino en la posibilidad de orientar el sistema hacia lo más conveniente, basado en principios propios del negocio y de la protección de la información, como activo fundamental de la organización. Es decir, un elemento que busca para conciliar la funcionalidad de los servicios con las regulaciones propias de las operaciones. En este sentido, se establece una promesa compartida entre los dueños del negocio, los profesionales de las tecnologías de información y los de seguridad informática: que los clientes puedan utilizar la potencialidad de las tecnologías, con la confiabilidad requerida y las medidas de protección establecidas de manera natural y efectiva."*

Para lo cual se necesita una correcta administración y contrapeso de controles, principalmente para que el área de Tecnología y Seguridad pueda desarrollar sus actividades y se encuentren alineados a los requerimientos del negocio.

9.4. La Ley N°20.488 de incumbencias profesionales y la administración del sistema de gestión de activos de información

En esta sección se analizarán los principales apartados existentes en la Ley de incumbencias de los profesionales en Ciencias Económicas, relacionadas a la profesión del Contador; y la gestión de activos de información en el ámbito de las entidades bancarias.

En el artículo N°13, la Ley N°20.488 establece que se requerirá el título de Contador Público o equivalente:

> *"en materia económica y contable cuando los dictámenes sirvan a fines judiciales, administrativos o estén destinados a hacer fe pública en relación con las siguientes cuestiones: "Elaboración e implantación de políticas, sistemas, métodos y procedimientos de trabajo administrativo–contable" y la "aplicación e implantación de sistemas de procesamiento de datos y otros métodos en los aspectos contables y financieros del proceso de información gerencial."*[xii] (Argentina, 2017)

En el citado artículo, se puede destacar la vinculación con la "*implantación de políticas, sistemas, métodos y procedimientos de trabajo administrativo – contable*". Partiendo de la base que en la actualidad se han desarrollado mejores prácticas y modelos de gestión que abarcan desde las normas IRAM/ISO de calidad, ambientales, Informe COSO, hasta el marco COBIT de ISACA; cada uno termina impactando en los sistemas de activos de información contable y es dónde el

contador puede contribuir en la planificación, gestión y control de diferentes sistemas administrativos.

En esta línea, algunas de las comisiones del Consejo Profesional en Ciencias Económicas de la Ciudad Autónoma de Buenos Aires, como la de Sistemas de Registros[xiii], plantean la necesidad de reconocer que los profesionales podrían (realizando las especializaciones correspondientes), implantar estándares de sistemas de gestión y liderar a las auditorías sobre las normas ISO, independientemente de la legal forma.

Para lo cual se necesitaría un profesional con una visión integral sobre estos temas, para encarar las diferentes cuestiones especificadas en las incumbencias profesionales del Contador Público.

9.5. Conclusiones particulares del capítulo IV

Por todo lo expuesto, se puede identificar al conjunto de personas y áreas abocadas a la gestión de activos de información en entidades bancarias. Las mismas pueden ser agrupadas de la siguiente forma:

- Área responsable de la administración del SAIC

- Áreas relacionadas con la gestión de activos de información

- Áreas de soporte en la gestión de los activos de información

- Áreas y personas usuarias de la información

Al analizar la normativa vigente, el BCRA dispuso en la Comunicación “A” 4609 que el área responsable de la gestión de los activos es denominada: “Protección de activos de información”. La misma “*será responsable de observar la existencia y correcta aplicación de los controles considerados como práctica recomendada y de uso frecuente en la implementación de la protección de los activos*” (BCRA, 2006).

Al analizar en general las incumbencias profesionales en Ciencias Económicas y en particular la del Contador Público, y contextualizado en la presente investigación, (en donde se describe un Marco Contable para los activos de información en las organizaciones bancarias) se puede identificar que la Ley N°20.488 se establecen como incumbencias del Contador Público: la elaboración e implantación de políticas, sistemas, métodos y procedimientos de trabajo administrativo – contable, como también la aplicación e implantación de sistemas de procesamiento de datos en los aspectos contables y financieros del proceso de información gerencial; relacionando a la profesión en los métodos de procesamientos y soportes que son el contexto de la información contable.

A continuación, se analizarán con las leyes propuestas para los sujetos existentes en la contabilidad y su contrastación con el modelo contable alternativo para los activos de información:

ESQUEMA N°36: Contrastación sobre los sujetos de la actividad contable

Leyes sobre personas y sujetos de la actividad contable enunciados por los autores CLGC, LFG y MCRDM.	Contrastación de las leyes en el contexto de la contabilización de activos de información.
1. Las diferencias que se observan entre individuos en materia de necesidades, habilidades y predisposición gravitan en la actividad contable y la hacen sumamente compleja.	En la contabilización de los activos de información se identifican individuos con habilidades específicas para el tratamiento de registración, control y resguardo de la información.
2. La diversidad de metas de los sujetos intervinientes influye en su tarea particular y condiciona la tarea contable.	En la contabilización de los activos de información se identifican individuos que desarrollan habilidades para resolver problemas sobre la actividad contable.
3. El que la actividad humana en sociedad no sea exclusivamente económica implica considerar metas sociales prioritariamente y resulta relevante para la actividad contable	En la contabilización de los activos de información se pueden identificar metas dispuestas por la legislación vigente, organismos de

en las organizaciones y para la regulación contable.	control y bajo los objetivos organizacionales.
4. La regulación contable se halla sumamente influida por las distintas metas (y por la variación de las mismas) de los individuos intervinientes.	La contabilización de los activos de información en entidades financieras se encuentra influida por las regulaciones impuestas por el Banco Central de la República Argentina y la legislación relacionada con Habeas Data.
5. Existen problemas de comunicación entre contadores prácticos y académicos, entre usuarios y emisores de informes y entre reguladores y revisores.	En la contabilización de los activos de información se identifican problemas de comunicación entre los usuarios y emisores de los informes y entre los reguladores y auditores.

Capítulo X

10. Informes contables no monetarios de activos de información en Entidades Bancarias

10.1. Introducción

En la contabilización de los activos de información en entidades bancarias se pueden identificar diversos informes internos y externos resultantes del sistema información objeto de estudio denominado “sistema de activos de información contable" (SAIC). A continuación, se detallan los informes contables relevados internamente en las entidades:

10.2. Informes Internos

Los informes internos identificados emitidos por los módulos del SAIC:

A. Informes suministrados sobre eventos del sistema de gestión de información y eventos de seguridad (SIEM):

- Reportes de seguridad que registren la asignación de claves y derechos de accesos.
- Reportes de seguridad de actividades de los usuarios privilegiados.
- Reportes de seguridad de usuarios de emergencia y con accesos especiales.
- Reportes de seguridad de intentos fallidos de acceso.
- Reportes de seguridad de bloqueos de cuentas de usuario.
- Reportes de auditoría que registren las excepciones y actividades críticas de las distintas plataformas.

B. Informes suministrados por el sistema de administración de gestión de bases de datos (CMDB).

C. Informes suministrados por el sistema de prevención de fuga de información (DLP).

D. Reportes de la gestión del inventario y clasificación de activos de información.

F. Informes sobre la gestión de incidentes se seguridad.

H. Indicadores de seguridad de la información (Tablero de comando). A continuación, se exponen los indicadores internos más relevantes para la protección de los activos de información en entidades bancarias.

ESQUEMA N°37: Indicadores estratégicos sobre seguridad y privacidad de la información

Objetivo del indicador	Característica de la métrica	Periodicidad
Calcular el porcentaje de los procesos de seguridad documentados de la organización.	Identificar el porcentaje de procesos de seguridad documentados en la entidad.	Semestral
Calcular el porcentaje de los instructivos de seguridad que conformen en los procesos de la entidad.	Identificar el porcentaje de actualización de políticas de seguridad.	Anual
	Identificar el porcentaje de actualización de normas de seguridad.	Anual
	Identificar el porcentaje de actualización de procedimientos de seguridad.	Anual
Calcular el porcentaje de documentación de procesos establecidos y de los futuros a implementar.	Identificar el porcentaje de procesos operativos de seguridad que están implementados.	Trimestral
Calcular el porcentaje de cumplimiento del sistema de control interno en los procedimientos inventariados.	Identificar el porcentaje de documentación normativa no analizada por normativas de control interno.	Semestral

ESQUEMA N°38: Indicadores estratégicos sobre capacitación y concientización de los recursos humanos

Objetivo del indicador	Característica de la métrica	Periodicidad
Calcular la efectividad del plan de concientización y concientización.	Identificar el porcentaje de personal que recibió inducción en seguridad desde su ingreso a la entidad.	Bimestral
	Identificar la cantidad de campañas a clientes referidas a buenas prácticas de seguridad y cuidado de la información.	Anual
	Identificar la periodicidad de envío de correo, mensajes; publicación de boletines y otros comunicados de concientización a empleados y clientes.	Trimestral
	Identificar la periodicidad de envío y publicación de boletines y otros comunicados de concientización a empleados y a clientes de la entidad.	Bimestral

ESQUEMA N°39: Indicadores estratégicos sobre los riesgos de los activos de información

Objetivo del indicador	Característica de la métrica	Periodicidad
Calcular la efectividad en la identificación de los dueños de activos de información en el proceso de análisis de riesgo de la entidad.	Identificar el porcentaje de dueños de activos que participaron en el proceso de análisis de riesgo.	Trimestral
	Identificar el porcentaje de activos cuyos dueños	Trimestral

	contestaron cuestionarios sobre madurez de los controles.	
	Identificar el porcentaje de activos de información clasificados o reclasificados anualmente por sus dueños.	Anual
	Identificar el porcentaje de activos de información cuyos dueños hayan sido notificados sobre incidentes de seguridad.	Trimestral
Calcular la efectividad de la documentación de los riesgos de los activos de información.	Calcular el porcentaje de procesos cubiertos en el análisis de riesgos sobre los planificados.	Trimestral
	Calcular el porcentaje de incremento de activos de información identificados respecto al período anterior.	Trimestral
	Calcular el porcentaje de activos de información que hayan cambiado su clasificación de un período al otro.	Anual
	Calcular el porcentaje de activos de información no analizados en la entidad.	Trimestral
	Calcular el porcentaje de activos con riesgo alto en el análisis general.	Trimestral
	Calcular el porcentaje de activos con riesgo medio en el análisis general.	Trimestral
	Calcular el porcentaje de activos con riesgo bajo en el análisis general.	Trimestral
Calcular la eficacia de los riesgos analizados y cuantificados	Calcular el porcentaje de vulnerabilidades con riesgo alto en el análisis total.	Trimestral

	Calcular el porcentaje de procesos críticos de negocio.	Mensual
	Calcular el porcentaje de procesos con alto nivel de riesgo incluidos en el plan de continuidad del negocio.	Semestral
Calcular la eficacia de los controles.	Calcular el porcentaje de controles correspondientes a la Comunicación “A” 4609 del BCRA que tengan grado de madurez inicial.	Trimestral
	Calcular el porcentaje de proyectos o iniciativas del área que hayan surgido del análisis de riesgos a los activos de información.	Anual

ESQUEMA N°40: Indicadores estratégicos sobre el cumplimiento normativo

Objetivo del indicador	Característica de la métrica	Periodicidad
Calcular el estado de las auditorías relacionadas al marco normativo de la seguridad de la información	Indicar la cantidad de observaciones de auditoría pendientes de resolución.	Semestral
	Indicar la cantidad de observaciones de auditoría pendientes de resolución sin un plan de remediación asociado.	Semestral
	Indicar la cantidad de observaciones de auditoría por incumplimiento normativo pendiente de resolución.	Semestral

ESQUEMA N°41: Indicadores estratégicos sobre información de gestión

Objetivo del indicador	Característica de la métrica	Periodicidad
Calcular la emisión de indicadores de gestión a través de un tablero de comando	Calcular la emisión continua de información en el tablero de comando.	Trimestral
	Calcular el porcentaje de informes y reportes de activos de información resultados reportados a la alta gerencia.	Trimestral

ESQUEMA N°42: Indicadores estratégicos sobre la arquitectura de seguridad

Objetivo del indicador	Característica de la métrica	Periodicidad
Calcular la participación en proyectos con aspectos de seguridad en las nuevas implementaciones de negocios y/o tecnológicas	Calcular el porcentaje de proyectos de negocios en donde participó el área de protección de activos	Anual
	Calcular el porcentaje de contratos de servicios de terceros analizados por el área de protección de activos	Anual
	Calcular el porcentaje de nuevos activos de información que pasaron para ser analizados previo a su producción.	Semestral
Calcular la tolerancia a fallas de infraestructura crítica	Calcular el porcentaje de disponibilidad de la infraestructura crítica de seguridad.	Mensual
	Calcular el tiempo de recuperación promedio ante fallas de infraestructura crítica.	Mensual

Calcular la documentación de los estándares de seguridad para las distintas plataformas.	Calcular el porcentaje de estándares de “hardening” definidos en relación con las plataformas utilizadas.	Semestral
Calcular la recurrencia de incidentes	Indicar la cantidad de incidentes recurrentes en los activos de información.	Mensual
Calcular la cantidad de incidentes críticos en los procesos de negocio	Indicar la cantidad de incidentes críticos que afectaron a procesos.	Mensual
	Indicar la cantidad de vulnerabilidades pendientes de corrección que involucran a sistemas críticos.	Mensual
Calcular la cantidad de vulnerabilidades identificadas	Indicar la cantidad de vulnerabilidades pendientes de corrección.	Mensual

ESQUEMA N°43: Indicadores estratégicos sobre los canales electrónicos

Objetivo del indicador	Característica de la métrica	Periodicidad
Calcular la cantidad de canales electrónicos de la entidad	Calcular el porcentaje de canales críticos que tienen activado el registro de eventos de seguridad.	Mensual
Calcular el grado de cumplimiento de la normativa oficial del BCRA para canales electrónicos.	Calcular el grado de cumplimiento de los requisitos establecidos en la Comunicación “A” 6017 del BCRA.	Trimestral

ESQUEMA N°44: Indicadores estratégicos sobre monitoreo y control

Objetivo del indicador	Característica de la métrica	Periodicidad
Calcular la efectividad del proceso de monitoreo.	Calcular el porcentaje de vulnerabilidades e incidentes detectados.	Mensual
	Calcular el porcentaje de controles implementados respecto al total planificado.	Mensual
	Indicar la cantidad de eventos críticos detectados no contemplados en el Sistema de Activos de Información Contable.	Mensual
	Calcular el porcentaje de usuarios críticos cuyos accesos son consistentes con el puesto funcional asignado.	Mensual
	Calcular el porcentaje de sistemas, servicios y/o aplicaciones críticas, para las cuales se realiza un control periódico de niveles y privilegios otorgados.	Mensual

A continuación, se exponen los indicadores tácticos y operativos más relevantes para la protección de los activos de información en entidades bancarias.

ESQUEMA N°45: Indicadores tácticos y operativos de riesgo de activos de información

Objetivo del indicador	Característica de la métrica	Periodicidad
Calcular la eficacia de la documentación de los riesgos de los activos de información.	Calcular el porcentaje de procesos de negocio críticos con un propietario identificado formalmente.	Trimestral
	Indicar la cantidad de activos de información no incluidos en los análisis de riesgos.	Trimestral
	Calcular el porcentaje de activos de información clasificados.	Trimestral
	Calcular el porcentaje de incidentes relacionados con un activo de información no inventariado.	Trimestral
	Calcular el porcentaje de incidentes críticos relacionados con amenazas o vulnerabilidades no identificadas en el análisis de riesgos.	Trimestral
	Calcular el grado de cumplimiento general normalizado con respecto a la Comunicación “A” 4609 del BCRA.	Trimestral

ESQUEMA N°46: Indicadores tácticos y operativos de gestión de incidentes

Objetivo del indicador	Característica de la métrica	Periodicidad
Calcular la eficacia del proceso de monitoreo.	Calcular el porcentaje de incidentes y vulnerabilidades comunicados dentro de un margen de tiempo establecido.	Mensual
	Calcular el porcentaje de incidentes y vulnerabilidades notificados a la gerencia o propietario de información.	Mensual
	Calcular el porcentaje de incidentes y vulnerabilidades conocidos y no reportados	Mensual
	Indicar la cantidad de vulnerabilidades pendientes de corrección que involucran a activos con alto nivel de riesgo	Mensual
	Calcular el porcentaje de activos de información que tienen activado el registro de eventos y se controla el envío de alertas.	Mensual
	Calcular el porcentaje de activos de información críticos alcanzados por el monitoreo y control.	Quincenal
	Indicar la cantidad de modificaciones injustificadas de configuración de pistas de auditoría.	Diaria
	Indicar la cantidad de casos detectados relacionados con la asignación de roles contrapuestos.	Mensual

	Indicar la cantidad de accesos injustificados a bases de datos.	Mensual
	Indicar la cantidad de usuarios que cuentan con algún tipo de acceso remoto injustificado.	Mensual
	Indicar la cantidad de usuarios que cuentan con acceso no controlado a bases de datos por fuera de las aplicaciones.	Mensual
	Indicar la cantidad de activos de información en los cuales está restringido el acceso a los servicios y la información de registro de eventos	Mensual

ESQUEMA N°47: Indicadores tácticos y operativos de administración de accesos

Objetivo del indicador	Característica de la métrica	Periodicidad
Calcular la eficacia del sistema de seguridad de la información.	Indicar la cantidad de accesos no autorizados detectados en un período de tiempo	Diaria
	Calcular el porcentaje de sistemas, servicios y/o aplicaciones cuyos archivos de contraseñas no cuenten con el nivel de protección.	Semestral
	Calcular el porcentaje de sistemas, servicios y/o aplicaciones cuyas políticas de usuario y contraseña estén alineadas con el BCRA.	Mensual
	Indicar la cantidad de modificaciones en configuración de política de contraseñas que no estén	Diaria

	alineadas con el estándar del BCRA.	
	Calcular el porcentaje de sistemas, servicios y/o aplicaciones críticas que cuenten con doble factor de autenticación para el acceso remoto.	Mensual
	Indicar la cantidad de aperturas injustificadas de sobres	Diaria
	Calcular el porcentaje de puestos funcionales para los cuales el otorgamiento y revocación de accesos se encuentran automatizados por medio de una herramienta.	Mensual
	Calcular el porcentaje de sistemas, servicios y/o aplicaciones, para los cuales el otorgamiento y revocación de accesos se encuentran automatizados por medio de una herramienta.	Mensual
	Indicar la cantidad de asignaciones injustificadas de usuarios especiales	Mensual
	Calcular el porcentaje de ejecuciones injustificadas de comandos sensitivos.	Mensual
	Calcular el porcentaje de actualizaciones injustificadas de tablas críticas.	Mensual
	Calcular el porcentaje de sistemas, servicios o aplicaciones críticos para los cuales el acceso concurrente se encuentra restringido.	Mensual

ESQUEMA N°48: Indicadores tácticos y operativos de fuga de información

Objetivo del indicador	Característica de la métrica	Periodicidad
Calcular la cantidad de medidas para la protección para evitar la fuga de información.	Calcular el porcentaje de alertas del DLP alcanzados por medidas contra la fuga de información.	Mensual
	Calcular el porcentaje de alertas del DLP sobre la extracción de información sensible.	Mensual
	Indicar la cantidad de casos en que información sensible fue detectada dentro de la entidad, pero fuera de la base de datos.	Mensual
	Indicar la cantidad de casos confirmados en que información sensible fue perdida o transferida a destinatarios no autorizados fuera de la entidad.	Mensual

ESQUEMA N°49: Indicadores tácticos y operativos de incidentes

Objetivo del indicador	Característica de la métrica	Periodicidad
Calcular la cantidad de incidentes	Calcular el porcentaje de activos no protegidos por un perímetro de seguridad física.	Mensual
	Indicar la cantidad de incidentes de seguridad física donde se permitió la entrada a personal no autorizado a las	Mensual

	instalaciones que contienen sistemas de información.	
	Calcular el porcentaje de activos críticos que no se encuentren en condiciones ambientales adecuadas.	Mensual
	Indicar la cantidad de incidentes de pérdida de disponibilidad ocasionados por factores ambientales.	Mensual
	Calcular el porcentaje de activos portables con medidas de protección adecuadas.	Mensual
	Indicar la cantidad de incidentes que afectaron a activos portables por falta de medidas de protección adecuadas.	Mensual
Calcular la efectividad de los mecanismos de detección, recuperación y prevención contra código malicioso.	Indicar la cantidad de activos retirados con fecha de depuración / destrucción vencida.	Mensual
	Calcular el porcentaje de equipos que tengan la última versión de parches de seguridad ya instalada	Mensual
	Calcular el porcentaje de parches de seguridad publicados implementados dentro de los tiempos definidos por la organización.	Mensual
	Indicar la cantidad de parches de seguridad pendientes de implementación por tipo de tecnología.	Mensual
	Calcular la antigüedad promedio de los parches de	Mensual

	seguridad pendientes de implementación.	
	Calcular el porcentaje de equipos con cobertura antivirus.	Mensual
	Calcular el porcentaje de equipos que tengan la última versión de antivirus ya instalada.	Mensual
	Calcular la antigüedad promedio de las actualizaciones de antivirus pendientes de implementación.	Mensual
	Indicar la cantidad de incidentes por falta de antivirus actualizado.	Mensual
	Calcular el porcentaje de equipos infectados respecto a la cantidad total de equipos.	Mensual
	Calcular el porcentaje de equipos con acceso denegado desde la red corporativa a sitios de Internet considerados peligrosos.	Mensual
	Indicar la cantidad de incidentes por acceso desde la red corporativa a sitios de Internet considerados peligrosos.	Mensual
	Calcular el porcentaje de equipos en los cuales está habilitada la instalación de software por parte de los usuarios.	Mensual
	Calcular el porcentaje de equipos detectados	Mensual

	conteniendo software no autorizado.	
	Indicar la cantidad de incidentes causados por la instalación de software no autorizado.	Mensual

10.3. Informes externos

Se identificaron los siguientes informes externos del “sistema de activos de información contable" (SAIC):

A. Informe sobre incidentes críticos al BCRA, (las entidades deben informar los incidentes críticos ocurridos por ciberataques o por seguridad de la información).

B. Informe anual sobre las bases de datos exigidos por la AAIP, con la criticidad de las Bases de Datos en el ámbito Nacional.

C. Informes a la Auditoría General del Gobierno de la Ciudad de Buenos Aires. En el caso de los bancos públicos en el ámbito de la CABA tienen que informar sobre la infraestructura de Software y Hardware. Datos que luego se utilizan para la confección de Informes Macrosociales del entorno de la CABA.

D. Informes sobre la contratación de servicios tercerizados críticos al BCRA, (En este caso las entidades deben informar los servicios tercerizados a la entidad).

E. Informes ISAE (Encargos de Aseguramiento) hacia terceros.

10.4. Conclusiones del capítulo X

En el dominio del discurso contable de los activos de información, se pueden identificar diferentes informes microsociales para usuarios internos y externos. En el siguiente esquema se representan las relaciones del SAIC con los reportes emitidos.

ESQUEMA N°50: Informes emitidos por el SAIC

Fuente: Elaboración propia.

Capítulo XI

11. Identificación de Normas Contables Legales para el sistema de activos de información

11.1. Introducción

En el presente capítulo se identificarán aquellas normas contables legales aplicables a la contabilización de activos de información en el ámbito de la Ciudad Autónoma de Buenos Aires.

11.2. Ley de protección de datos personales

11.2.1. Introducción

En el año 2000, en la República Argentina se promulgó la Ley N°25.326 de Protección de Datos Personales, en donde se estableció entre otras obligaciones, que las bases de datos o archivos públicos y privados destinados a proporcionar informes deben estar inscriptos en un registro especial.

En los sistemas de registros contables de las organizaciones "*existen numerosas bases de datos que contienen y analizan información personal, emitiendo diferentes tipos de informes cuyos archivos deberían estar registrados para cumplir con el marco legal vigente*." (Escobar, Ley de Protección de Datos Personales, 2010).

En este capítulo, se analiza la Ley de Protección de Datos personales y su vinculación con los activos de información en las entidades bancarias.

11.2.2. Reconocimiento de las bases de datos presentes en las organizaciones. Conceptos y objetivos de la Ley N°25.326

El principal objetivo de la ley es la *"protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como el acceso a la información que sobre las mismas se registre."* (Escobar, Ley de

Protección de Datos Personales, 2010). La ley toma en cuenta tanto los datos de las personas físicas como los de las personas jurídicas.

A continuación, se analizan las secciones más relevantes de la ley, prestando mayor interés a la emisión y conservación de comprobantes comerciales.

11.2.3. Clasificación de datos personales

La Ley N°25.328 y las Disposiciones de la Agencia de Acceso a la Información Pública (AAIP), ex - Dirección Nacional de Protección de Datos Personales (exDNPDP), *"han establecido una clasificación a los datos personales, en datos básicos, intermedios y sensibles"* (Suarez Kimura & Escobar, Repercusiones de La Ley De Protección de Datos Personales en el Ejercicio Profesional del Contador Público, 2010). Como se indicó precedentemente, la misma es considerada una de las metodologías de medición de los activos de información. Los datos considerados básicos, corresponden a los presentes en el padrón electoral. Los datos sensibles son datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. Y los datos intermedios son los que superan a los básicos y no son sensibles.

Con respecto a la categoría de datos, el artículo N°7 de la Ley establece que:

"1. Ninguna persona puede ser obligada a proporcionar datos sensibles.

2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.

4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades competentes, en el marco de las leyes y reglamentaciones respectivas." (Congreso de la República Argentina, 2020)

A continuación, se presenta la documentación presente en las empresas, en donde se incluyen datos personales, con la clasificación de la información contenida.

ESQUEMA N°51: Comprobantes y documentación bancaria

Tipo de Comprobante	Características	Tipo de Dato
Facturas	Si determina el cliente	Datos Intermedios
Notas de Débito	Si determina el cliente	Datos Intermedios
Notas de Crédito	Si determina el cliente	Datos Intermedios

Remitos	Si determina el cliente	Datos Intermedios
Cupones de Tarjeta de Crédito / Debito	Si determina el cliente	Datos Intermedios
Fuente: Elaboración propia.		

ESQUEMA N°52: Comprobantes internos bancarios

Tipo de Comprobante	Características	Tipo de Dato
Todo tipo de comprobante bancario	Si determina el Cliente	Datos Intermedios
Legajos de Clientes	Si determina el Cliente	Datos Intermedios
Asientos Diarios	-	Datos Intermedios
Papeles de Trabajo que determinan Clientes.	-	Datos Intermedios
Fuente: Elaboración propia.		

La información contenida en los comprobantes y documentación bancaria con "*la identificación de los clientes o proveedores es considerada intermedia porque con los datos contenidos en los mismos se pueden determinar el ingreso y el consumo de estos, su capacidad de pago y su disponibilidad, entre otras cosas"* (Suarez Kimura & Escobar, 2017)

Con respecto a las bases de datos existentes en las entidades, se encontraron las siguientes:

ESQUEMA N°53: Relacionados con los empleados

Tipo de Comprobante	Tipo de Dato
Legajos Personales	Datos Sensibles
Recibos de Sueldos y Jornales	Datos Intermedios
Declaraciones Juradas	Datos Intermedios
Formularios de Contribuciones Sociales	Datos Sensibles
Fuente: Elaboración propia.	

ESQUEMA N°54: Relacionados con clientes y proveedores

Tipo de Comprobante	Características	Tipo de Dato
Bases de productos activos y pasivos	Si determina el cliente	Datos Intermedios
Facturas, Nota debito / Crédito, Remitos, etc.	Si determina el cliente	Datos Intermedios
Fuente: Elaboración propia.		

En el caso de las bases de datos con información de sus empleados, están conformadas por datos intermedios y sensibles, que son utilizados para confeccionar declaraciones juradas, realizar aportes y contribuciones, asignaciones familiares, entre otros.

Como se aclaró precedentemente, en las organizaciones existen numerosas bases de datos con la información personal para confeccionar diversos informes, que tendrían que estar registradas en la AAIP. No se debería considerar únicamente

como una obligación, sino también como una ventaja competitiva en el manejo de la información.

11.2.4. Seguridad de los datos

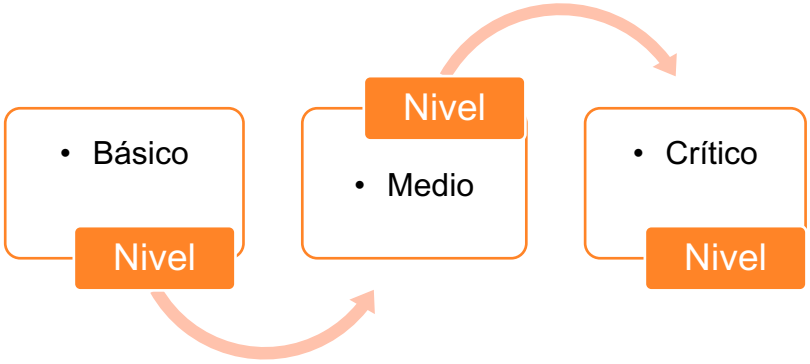
El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad, seguridad, como también los que no garanticen el cumplimiento de los términos de la presente ley.

En la disposición N°11/2006, la AAIP, establece diferentes niveles de seguridad, para el tratamiento y conservación de los datos personales contenidos en archivos, registros, bancos y bases de datos públicas no estatales y privadas. Dichos niveles de seguridad dependen del tipo de datos que contengan.

A continuación, se enunciarán las características más importantes de cada nivel de seguridad. (AAIP, 2020)

ESQUEMA N°55: Niveles de Seguridad



Fuente: Elaboración propia.

11.2.4.1. Medidas de seguridad del nivel básico

Para los archivos, registros, bases y bancos de datos que contengan datos de carácter personal, deberán adoptarse las medidas de seguridad calificadas como de nivel básico en la disposición N°11/2006 (AAIP, 2020) que a continuación se detallan:

Disponer del documento de seguridad de datos personales en el que se especifiquen, entre otros, los procedimientos y las medidas de seguridad a observar sobre los archivos, registros, bases y bancos con contenidos de estas características. Deberá mantenerse en todo momento actualizado y ser revisado cuando se produzcan cambios en el sistema de información.

Contendrá, entre otras, las siguientes medidas:

ESQUEMA N°56: Medidas de seguridad del nivel básico
1. "Funciones y obligaciones del personal".
2. "Descripción de los archivos con datos de carácter personal y los sistemas de información que los tratan".
3. "Descripción de las rutinas de control de datos de los programas de ingreso de datos y las acciones a seguir ante los errores detectados a efectos de su corrección. Todos los programas de ingreso de datos, cualquiera sea su modo de procesamiento (batch, interactivo, etc.), deben incluir en su diseño, rutinas de control, que minimicen la posibilidad de incorporar al sistema de información, datos ilógicos, incorrectos o faltantes".
4. "Registros de incidentes de seguridad".
5. "Procedimientos para efectuar las copias de respaldo y de recuperación de datos".
6. "Relación actualizada entre Sistemas de Información y usuarios de datos con autorización para su uso".
7. "Procedimientos de identificación y autenticación de los usuarios de datos autorizados para utilizar determinados sistemas de información".
8. "Control de acceso de usuarios a datos y recursos necesarios para la realización de sus tareas para lo cual deben estar autorizados".

9. "Medidas de prevención a efectos de impedir amenazas de software malicioso (virus, troyanos, etc.) que puedan afectar archivos con datos de carácter personal".
Fuente: Disposición N°11/2006 – (AAIP, 2020)

11.2.4.2. Medidas de seguridad del nivel medio

Además de las medidas de seguridad de nivel básico, deberán adoptarse las que se detallan a continuación sobre los archivos, registros, bases y bancos de datos de las empresas privadas que desarrollen actividades de prestación de servicios públicos, así como los pertenecientes a entidades que cumplan una función pública y/o privada que, más allá de lo dispuesto por el artículo N°10 de la Ley N°25.326, deban guardar secreto de la información personal por expresa disposición legal (como el secreto bancario):

ESQUEMA N°57: Medidas de Seguridad del Nivel Medio
1. "El Instructivo de seguridad deberá identificar al responsable (u órgano específico) de Seguridad".
2. "Realización de auditorías (internas o externas) que verifiquen el cumplimiento de los procedimientos e instrucciones vigentes en materia de seguridad para datos personales".

3. “Limitar la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información”.
4. “Establecer un control de acceso físico a los locales donde se encuentren situados los sistemas de información con datos de carácter personal”.
5. “Gestión de Soportes e información contenida en ellos”.
6. “Los registros de incidentes de seguridad, en el caso de tener que recuperar datos, deberán identificar la persona que recuperó y/o modificó dichos datos. Será necesaria la autorización en forma fehaciente del responsable del archivo informatizado”.
7. “Las pruebas de funcionamiento de los sistemas de información, realizadas con anterioridad a su puesta operativa, no se realizarán con datos/archivos reales, a menos que se aseguren los niveles de seguridad correspondientes al tipo de datos informatizados tratados”.
Fuente: Disposición N°11/2006 – (AAIP, 2020)

11.2.4.3. Medidas de seguridad del nivel crítico

Los archivos, registros, bases y bancos de datos que contengan datos personales, definidos como "datos sensibles", además de las medidas de seguridad de nivel básico y medio, deberán adoptar las que a continuación se detallan:

ESQUEMA N°58: Medidas de Seguridad de Nivel Crítico
*1. "**Distribución de soportes**: cuando se distribuyan soportes que contengan archivos con datos de carácter personal —incluidas las copias de respaldo—, se deberán cifrar dichos datos (o utilizar cualquier otro mecanismo) a fin de garantizar que no puedan ser leídos o manipulados durante su transporte."*
*2. "**Registro de accesos**: se deberá disponer de un registro de accesos con información que identifique al usuario que accedió, cuándo lo hizo (fecha y hora), tipo de acceso y si ha sido autorizado o denegado. En el caso que el acceso haya sido autorizado se deberá identificar el dato accedido y el tratamiento que se le dio al mismo (baja, rectificación, etc.). Este registro de accesos deberá ser analizado periódicamente por el responsable de seguridad y deberá ser conservado como mínimo por el término de un TRES (3) años."*
*3. "**Copias de respaldo**: además de las que se mantengan en la localización donde residan los datos deberán implementarse copias de resguardo externas, situadas fuera de la localización, en una caja ignífuga y a prueba de gases o bien en una caja de seguridad bancaria, cualquiera de ellas situadas a prudencial distancia de la aludida localización. Deberá disponerse de un procedimiento de recuperación de esa información y de tratamiento de la misma en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales."*

*4. "**Transmisión de datos**: los datos de carácter personal que se transmitan a través de redes de comunicación deberán serlo cifrados o utilizando cualquier otro mecanismo que impida su lectura y/o tratamiento por parte de personas no autorizadas."*
Fuente: Disposición N°11/2006 – (AAIP, 2020)

Juntamente con la registración de las bases de datos con información personal, las entidades bancarias deben implementar el nivel de seguridad acorde con el tipo de datos que manejen, cabe destacar que el incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en la ley.

11.3. Identificación de medidas de control establecidas para resguardar los activos de información en custodia de las entidades bancarias privadas en el ámbito de la Ciudad Autónoma de Buenos Aires

11.3.1. Introducción

En el artículo Nº322 del nuevo Código Civil y Comercial, se establecen como registros indispensables, al "*diario, inventario y balances; aquellos que corresponden a una adecuada integración de un sistema de contabilidad y que exige la importancia y la naturaleza de las actividades a desarrollar; y a los que en*

forma especial impone este Código u otras leyes." (Congreso de la Nación Argentina, Código Civil y Comercial, Artículo N° 322, 2014).

Con relación a los sistemas de registros informatizados, el código establece que el titular puede, (previa autorización del Registro Público de su domicilio):

> *"a. sustituir uno o más libros, excepto el de Inventarios y Balances, o alguna de sus formalidades, por la utilización de ordenadores u otros medios mecánicos, magnéticos o electrónicos que permitan la individualización de las operaciones y de las correspondientes cuentas deudoras y acreedoras y su posterior verificación;*
>
> *b. conservar la documentación en microfilm, discos ópticos u otros medios aptos para ese fin. La petición que se formule al Registro Público debe contener una adecuada descripción del sistema, con dictamen técnico de Contador Público e indicación de los antecedentes de su utilización. Una vez aprobado, el pedido de autorización y la respectiva resolución del organismo de contralor, deben transcribirse en el libro de Inventarios y Balances.*
>
> *La autorización sólo se debe otorgar si los medios alternativos son equivalentes, en cuanto a inviolabilidad, verosimilitud y completitud, a los sistemas cuyo reemplazo se solicita."* (Congreso de la Nación Argentina, Código Civil y Comercial, Artículo N° 329, Actos sujetos a autorización, 2014)

En este artículo se establece que pueden llevarse en "*ordenadores u otros medios mecánicos, magnéticos o electrónicos",* sin prohibir utilización de un servicio de computación en la nube, pero con la previa autorización del Registro Público. Asimismo, se menciona la necesidad de contar con un *dictamen técnico de*

Contador Público y que la autorización sólo se debe otorgar si los medios alternativos son equivalentes, en cuanto a ***inviolabilidad, verosimilitud y completitud,*** a los sistemas cuyo reemplazo se solicita, alineado a lo exigido por la doctrina contable.

En la actualidad las entidades financieras del ámbito privado poseen sistemas de registros en medios tecnológicos y deben cumplir con los requisitos exigidos por los organismos de control en cada jurisdicción. En el presente capítulo se analizarán todos los requisitos establecidos por la IGJ que debe cumplir la información contable digitalizada.

11.3.2. Requisitos exigidos al sistema de información contable

La IGJ en la Resolución General N°7 de 2015, establece que los sistemas de registros contables deben cumplir con los requisitos enunciados a continuación:

ESQUEMA N°59: Tabla con los requisitos de los sistemas contables (IGJ)

Requisitos de los Sistemas Contables (IGJ)
1. "Se lleven mediante los registros contables necesarios para disponer de un sistema de contabilidad orgánico, adecuado a la importancia y naturaleza de las actividades del ente."

2. “Los registros contables tengan una denominación inequívoca y concordante con la función que cumplan y se evite la superposición de registros que contengan información similar y puedan inducir a confusión.”
3. “Ofrezcan elevado grado de inalterabilidad de las registraciones volcadas, el que estará sustentado en controles internos de tipo administrativo contable y otros de tipos operativos o programados, aplicables sobre la información de entrada, su procesamiento e información de salida. Dicha inalterabilidad buscará impedir que se genere más de un proceso de registración por cada hecho económico y que, asimismo, toda anulación de cualquier proceso se logre a través de un asiento de ajuste.”
4. “Permitan determinar la evolución y situación del patrimonio, incluyendo los resultados obtenidos, individualizar los registros y datos de análisis en que se basan los informes contables y su correlación con los documentos o comprobantes respaldatorios y localizar éstos a partir de los registros contables y viceversa, para lo cual los primeros deberán ser archivados en forma metódica que facilite la interrelación.”
5. “Permitan obtener acceso como parte de la operatoria habitual, debiendo estar respaldado por normas escritas aprobadas por el órgano de administración de la sociedad y copiadas en el libro de Inventarios y Balances o en un libro especial que cumpla con los requisitos formales

impuestos por el Código Civil y Comercial de la Nación, leyes complementarias y especiales, así como lo requerido por estas Normas."

Fuente: **(Inspección General de Justicia, 2020)**

Teniendo en cuenta estas características principales se analizan las diferentes cuestiones que deben cumplirse para resguardar la información contable de entidades bancarias en un contexto tecnológico.

11.3.3. Condiciones de los sistemas de registración contable resguardados en medios tecnológicos

La utilización de los sistemas de registros contables en medios de almacenamiento electrónicos como: *"compact disc, discos ópticos y microfilmes, ya sean microfichas o rollos"*[xiv] (Inspección General de Justicia, 2020), etc.), debe ajustarse a los siguientes requerimientos:

- ✓ **Existencia de un sistema de numeración de los medios de almacenamiento.**

Los elementos utilizados como soporte de almacenamiento deberán ser numerados correlativamente desde el número uno (1) en adelante (Inspección General de Justicia, 2020), para cada registro y por cada ejercicio económico, sin perjuicio del número de identificación de origen que les corresponda.

- ✓ **Cumplimiento de las características del soporte de almacenamiento de los registros contables.**

La información almacenada en el medio de soporte no podrá ser eliminada ni reescrita, debiendo poder ser leída la cantidad de veces que fuere necesario, sin deteriorarse. (Inspección General de Justicia, 2020) En el caso de la utilización de CDs y DVDs como medio de almacenamiento, no se deberían utilizar los regrabables.

- ✓ **Calidad del soporte de almacenamiento de los registros contables.**

Los medios de registro deberán cumplir con patrones de calidad e inalterabilidad que "impidan cualquier alteración a la información guardada y permitan su conservación" (Inspección General de Justicia, 2020) por el período de exigencia legal.

- ✓ **Establecimiento de controles internos a implementar en la operatoria de almacenamiento.**

La emisión de los soportes señalados deberá ser factible de obtenerse como parte de la operatoria habitual, debiendo los mismos estar "respaldados por normas escritas aprobadas por el órgano de administración de la sociedad y copiadas en el libro de Inventarios y Balances." (Inspección General de Justicia, 2020)

- ✓ **Demostración técnica del grado de inalterabilidad.**

En la normativa se establece que se debe demostrar “el grado de inalterabilidad de las registraciones a efectuar mediante el sistema propuesto” (Inspección General de Justicia, 2020), con lo cual se debería realizar una auditoría de la Seguridad de la Información del sistema contable para corroborar como mínimo las cuestiones enunciadas en el siguiente cuadro:

ESQUEMA N°60: Análisis de los requisitos de la Seguridad de la Información en el sistema contable

Requisitos de la Seguridad de la Información en el sistema contable		
Número	Descripción	Aclaraciones mínimas
1	Plataforma de Hardware utilizada.	Si el Hardware utilizado se corresponde con el nivel de transacciones de la operatoria de la empresa. Si se cambiaran los soportes, se debería poder consultar los registros anteriores en cualquier momento si así fuera requerido.[xv]
2	Plataforma de Software de Base y Aplicaciones utilizadas.	La correcta instalación y actualización del Software utilizado, con herramientas debidamente instaladas.
3	Políticas de Gestión de Seguridad informática	Las políticas de seguridad implementadas.
4	Control de Accesos Lógicos y Físicos	Análisis de los Controles de Accesos Lógicos y Físicos implementados.
5	Back-up / Archivo de la	La política de copias de respaldo y su correcta comprobación.

	documentación respaldatoria / Plan de contingencia	
6	Pautas de Confiabilidad.	Análisis de las pautas de confidencialidad con los empleados Implementadas.
7	Integridad de los Registros Contables	Comprobación de la utilización de Funciones de Hash para garantizar la inalterabilidad de los registros en los diferentes soportes.
Fuente: Elaboración Propia. (Inspección General de Justicia, 2020)		

También se establecen las particularidades que deben contener las actas de registración de los sistemas contables en formato tecnológico. La información contable por incluir deberá contener:

- ✓ Número de acta inicial y final.
- ✓ Número de identificación del soporte.
- ✓ Cantidad de registros en él contenida.
- ✓ Período que corresponde. (Inspección General de Justicia, 2020)

Además, se debe cumplir con los siguientes requisitos con las actas señaladas:

- ✓ “Deben ser firmadas por el representante legal de la sociedad”, y

✓ “Trimestralmente, el órgano de fiscalización verificará el cumplimiento de las condiciones señaladas en los que anteceden, emitiendo al respecto un informe especial que se registrará con su firma en el libro de Inventarios y Balances o en el libro de medios ópticos si lo hubiere. Trimestralmente, el órgano de fiscalización verificará el cumplimiento de las condiciones señaladas en los incisos que anteceden, emitiendo al respecto un informe especial que se registrará con su firma en el libro de Inventarios y Balances.” (Inspección General de Justicia, 2020)[xvi]

11.3.4. Trámites y requisitos solicitados por la Inspección General de Justicia (Resolución General N°7 de 2015)

Para iniciar el trámite de autorización para el empleo de ordenadores se deben cumplir con los siguientes elementos:

- Primer testimonio de escritura pública o instrumento privado original con los recaudos del artículo N°37, incisos N°1 y 2.
- Informe de las características del sistema
- Dictamen de precalificación de Contador Público

En el siguiente cuadro se especifican cada uno de ellos:

ESQUEMA N°61: Autorización para empleo de ordenadores (IGJ)		
Elementos	**Características**	**Notas**
Primer testimonio de escritura pública o instrumento privado original con los recaudos del artículo N°37, incisos N°1 y 2, conteniendo la transcripción de la resolución del órgano de administración de la sociedad, de solicitar la autorización reglamentada en este artículo. La resolución del órgano de administración deberá contener:	"a. En el caso de sustitución de libros rubricados, la denominación exacta de los libros rubricados que se reemplazan y registros que se solicitan; b. En el caso de sustitución de autorizaciones previamente emitidas por este Organismo de acuerdo con las disposiciones del artículo N°61 de la Ley N°19.550: Número de autorización que se reemplaza y registros por los que se efectúa la presentación. En caso de tratarse de una sustitución parcial, se indicarán los registros que continúan manteniéndose mediante la autorización ya emitida; c. El sistema de archivo a utilizar (medios ópticos, mecánicos u otros); d. La declaración expresa si el sistema y registros por los que se solicita autorización, han sido utilizados previo a la intervención del Organismo, indicando en su caso fecha de comienzo de utilización; e. Si se solicita la autorización de sistema en compact disc, otros discos ópticos y microfilmes, ya sean microfichas o rollos, deberá contener expresamente el compromiso de preservar la posibilidad de lectura de los medios de registración y/o extender en listados de papel los registros, durante el período en que la ley determina obligatoria su exigibilidad; f. En caso de tercerización de archivo de documentación física y/o informática, deberá contener la denominación del tercero proveedor del servicio, radicación de los archivos y/o medio de procesamiento, vigencia	Para el desarrollo de esta actividad se requieren los conocimientos de un Contador Público.

	del contrato y las políticas de seguridad en la información implementadas. g. Si el sistema de registración contable solicitado fuera de propio desarrollo, deberá surgir claramente la descripción del sistema, sus funciones, interfaces con las que opera y diagrama de módulos de conformidad con los requisitos dispuestos en el artículo N°326 de esta Norma, de modo tal que permitan la verificación prevista por el artículo N°335.”	
2. Las siguientes piezas firmadas por el representante legal o apoderado con facultades suficientes y por contador público independiente con su firma legalizada por la entidad que detenta la superintendencia de su matrícula, conteniendo:	“a. La exposición amplia y precisa del sistema de registración contable a utilizar, indicando los propósitos de la modificación propuesta; si se trata de la modificación o sustitución de un sistema anterior, deberán explicarse los motivos y las diferencias con el mismo. Debe incluirse la denominación exacta de los registros que se llevarán mediante el sistema y la de los libros que se reemplazan. b. Flujograma exponiendo el circuito administrativo–contable completo. Deben surgir claramente los datos que ingresan a partir de la documentación contable (facturas de compras, ventas, ingresos, egresos, etc.), su procesamiento y la salida que genera, la cual será coincidente con todos los registros contables de la sociedad. De existir interfaces, conexiones remotas u otras similares deberá exponerse en el diagrama. c. Demostración técnica del grado de inalterabilidad de las registraciones a efectuar mediante el sistema propuesto; indicando software y hardware a utilizar, política de contraseñas, conexiones remotas, interfaces, etc.	Para el desarrollo de esta actividad la norma requiere los conocimientos de un Contador Público matriculado, pero sería adecuado un experto en tecnología de la Información y Seguridad de la información.

d. Metodología de generación de CD o DVD y metodología de archivo de documentación respaldatoria y de los soportes. En el caso de microfilms, CD o DVD se requiere archivo ignífugo. e. El sistema y periodicidad en la numeración de los registros. f. Estado de actualización de todos los registros, contables y legales autorizados a la fecha de la presentación, indicando sus datos y fecha de rúbrica o autorización y la fecha y folio de la última registración practicada. Dicho estado de actualización se presentará con un atraso que no supere los treinta (30) días; g. Modelos en blanco por duplicado y uno ejemplificativo conteniendo: denominación social y domicilio legal inscripto, denominación del registro o listado, ambos configurados con fecha y número de página sin determinar. h. Plan de cuentas incluyendo denominación y domicilio social inscripto.”	
3. Dictamen de precalificación de contador público, en el cual se verificará: a. la situación de la sociedad en relación con todos los supuestos de los art. 94 y 299 de la Ley N°19.550, así como el cumplimiento detallado de los artículos 326, 333, 334 y 335 (según corresponda), quórum y mayorías de la reunión del órgano de administración. b. En el caso de sustitución de libros llevados bajo la modalidad de rúbrica y considerando las disposiciones del artículo N°342, informará si se ha previsto la solicitud de los libros necesarios para efectuar la discontinuación inmediata una vez emitida la autorización por parte de este Organismo, manteniendo la contabilidad actualizada a esa fecha. c. Radicación del archivo de la documentación respaldatoria y de los soportes.	Se requiere el título de Contador Público.

Elaboración propia del cuadro. Fuente: **(Inspección General de Justicia, 2020)**

Una vez aprobado el trámite de autorización hay que cumplir con los siguientes informes dispuestos por la IGJ:

- Informe Anual.
- Informe de actualización técnica.
- Otros que requiera el organismo.

En el siguiente cuadro se especifican las características más relevantes de los mismos:

ESQUEMA N°62: Informes periódicos medios magnéticos u otros.

Informes	**Características**	**Profesionales**
- 1 - Información anual; certificación.	Las sociedades que obtengan la autorización requerida por el artículo N°61 de la Ley N°19.550, deberán a partir del ejercicio económico de cierre inmediato siguiente a ella, dentro de los ciento veinte (120) días de cada cierre, presentar a la Inspección General de Justicia: **1.** Informe especial suscripto por contador público independiente, conteniendo: a. La descripción exacta del sistema utilizado durante el ejercicio económico. Se informará si se han implementado actualizaciones al sistema oportunamente aprobado, con indicación de versión original y versión actual, así como fecha de efecto. b. Opinión fundada sobre la concordancia existente entre el sistema de registración contable y diseño de registros utilizado	Se requiere el título de Contador Público.

durante dicho ejercicio y el oportunamente autorizado.

c. Informará datos del libro Inventario y Balances en el que se ha transcripto las autorizaciones y/o bajas emitidas por el Organismo, la descripción de los sistemas aprobados, los diseños de registros y el plan de cuentas.

d. En caso de detectarse discordancias entre el o los sistemas y diseños aprobados por el Organismo y los utilizados durante el ejercicio que se informa, el profesional interviniente acompañará detalle de las mismas, indicando fecha de efecto de cada una.

e. Informará opinión sobre cumplimiento de todos los apartados del artículo N°326, 333 y/o 334, según corresponda.

f. Junto con su informe, acompañará datos de la totalidad de los listados o registros utilizados durante el período que se informa, indicando: denominación, período, número inicial y final de cada soporte, libro o ficha y metodología de archivo de los mismos. En caso de medios ópticos indicará cumplimiento del artículo N°334, incisos N°5 y 6.

g. Informará vigencia del contrato de tercerización de archivo de documentación física y/o informática, en caso de corresponder.

2. Escrito debidamente suscripto por representante legal de la misma, con firma y cargo certificados notarialmente, invocando carácter de la presentación efectuada y ratificando la documentación acompañada por el profesional interviniente.

3. Copia/s de la autorización/es vigente/s para el ejercicio económico respectivo y copia de las actas labradas en cumplimiento de los incisos N°5 y 6 del artículo N°334 de estas Normas. De no existir observaciones se emitirá a la sociedad una certificación que lo indicará, la cual deberá ser agregada al libro de Inventarios y Balances. En el supuesto que en oportunidad del presente se verifique

	algún incumplimiento a las normas contenidas en el presente Título, la sociedad deberá regularizar su situación dentro de los noventa (90) días a contar desde la emisión de la constancia extendida por el Organismo.	
- II - Informe de actualización técnica. Sin perjuicio de la información a presentar conforme al apartado anterior, cada dos (2) años las sociedades deberán presentar:	**1.** Informe técnico emitido por contador público independiente sobre la situación de obsolescencia del sistema utilizado y, en su caso, un proyecto de actualización técnica del mismo y de las medidas y reemplazos necesarios, requiriendo nueva autorización conforme a lo dispuesto en el artículo N°328 anterior. Asimismo, dicho informe contendrá: a. Opinión fundada sobre la situación de obsolescencia del sistema oportunamente aprobado y estado de actualización técnica del mismo. b. Período bienal por el que se emite dicho informe. El mismo abarcará dos (2) ejercicios económicos y deberán ser coincidentes, cronológicamente, con los presentados en cumplimiento de la información anual requerida por el apartado I de este artículo. c. Datos del libro Inventario y Balances en el que se han transcripto las autorizaciones y/o bajas emitidas por el Organismo, la descripción del/ los sistemas aprobados, los diseños de registros y planes de cuentas. **2.** Escrito debidamente suscripto por representante legal de la misma, con firma y cargo certificados notarialmente, invocando carácter de la presentación efectuada y ratificando la documentación acompañada por el profesional interviniente. **3.** Copia/s de la autorización/es vigente/s y/o bajas para el período bienal respectivo.	Se requiere el título de Contador Público.
- III - Otros Informes	La Inspección General de Justicia podrá reglamentar el cumplimiento de recaudos adicionales, incluida la exigencia de que, si su volumen lo justificare, el movimiento contable de la sociedad sea volcado a soporte papel. La infracción a lo dispuesto en el presente artículo hará pasible a la	Se requiere el título de Contador Público.

sociedad, sus directores y síndico de hasta el máximo de la multa prevista en las leyes 19.550 y 22.315.
Fuente: **(Inspección General de Justicia, 2020)**

- **Profesionales comprometidos en los informes:**

En la Resolución General N°7/15 de la IGJ se especifica que el Informe Anual, el Informe de actualización técnica y los otros que requiera el organismo; deben estar acompañados del formulario correspondiente y un informe de un Contador Público con la firma legalizada por el organismo con poder de policía de la profesión. Bajo esta situación, surge la necesidad de contar con profesionales capacitados para comprender la problemática y trabajar interdisciplinariamente con especialistas en tecnología y seguridad y responder a estas demandas.

11.4. Conclusiones particulares del capítulo XI

En los sistemas de las entidades bancarias existen numerosas bases de datos en donde se almacena información relacionada con clientes, proveedores y empleados. La Ley N°25.326 establece que las destinadas a proporcionar informes o procesen información con datos personalizados deben inscribirse en el registro que al efecto habilite el organismo de control.

La información contenida en los sistemas contables no es exclusivamente para uso interno, ya que las entidades utilizan estos datos para realizar diversos reportes como: Estados Financieros, reportes a los organismos de control, informes sobre

responsabilidad social empresaria, marketing, etc., que son distribuidas a usuarios, sucursales o al holding al cual pertenecen.

La ley plantea que todas las bases de datos están sujetas al reglamento de esta ley, pero la AAIP aconseja registrar las bases de datos que tengan un impacto significativo en la sociedad.

Juntamente con la registración de las bases de datos con información personal, las empresas deben adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, a fin de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Las Entidades financieras del ámbito privado poseen sistemas de registros en medios tecnológicos y deben cumplir con los requisitos exigidos por los organismos de control en cada jurisdicción. Para las que se encuentran radicadas en la CABA, la Inspección General de Justicia describe rigurosas características para dar cumplimiento a la legal forma.

En la Resolución General N°7 del año 2015 se enuncian los requisitos que debe emplearse para la información financiera existente en las entidades bancarias bajo el control de la IGJ. Para obtener la autorización hay que cumplir con los siguientes requisitos relacionados con la seguridad de la información:

- La exposición amplia y precisa del sistema de registración contable a utilizar. Debe incluirse la denominación exacta de los registros que se llevarán mediante el sistema y la de los libros que se reemplazan; y

- Demostración técnica del grado de inalterabilidad de las registraciones a efectuar mediante el sistema propuesto;

Para garantizar la ***inviolabilidad, verosimilitud y completitud*** del sistema de registros se deben analizar los siguientes puntos de control sugeridos en el capítulo:

- Plataforma de Hardware utilizada.

- Plataforma de Software de Base y Aplicaciones utilizadas.

- Políticas de Gestión de Seguridad de la Información.

- Control de Accesos Lógicos y Físicos.

- Back-up / Archivo de la documentación respaldatoria.

- Plan de contingencia.

- Pautas de Confiabilidad.

- Integridad de los Registros Contables.

Capítulo XII

12. Identificación de normas y estándares para el control de los activos de información

12.1. Introducción

En la descripción del dominio del discurso contable de activos de información, resulta necesario identificar las normas o estándares existentes en la relacionadas con cada nivel de activo de información.

Para identificar el dominio del discurso contable en un modelo particular, resulta indispensable identificar las normativas aplicables y estándares utilizados en la contabilización y administración de los activos.

12.2. Control de los activos de información en custodia de las entidades bancarias: Identificación de mejores prácticas y estándares de control

12.2.1. Introducción

El objetivo de la presente sección es analizar e identificar aquellos marcos de gestión y buenas prácticas de Tecnología y Seguridad de la Información existentes en las entidades bancarias para la gestión de los activos de información bajo su custodia.

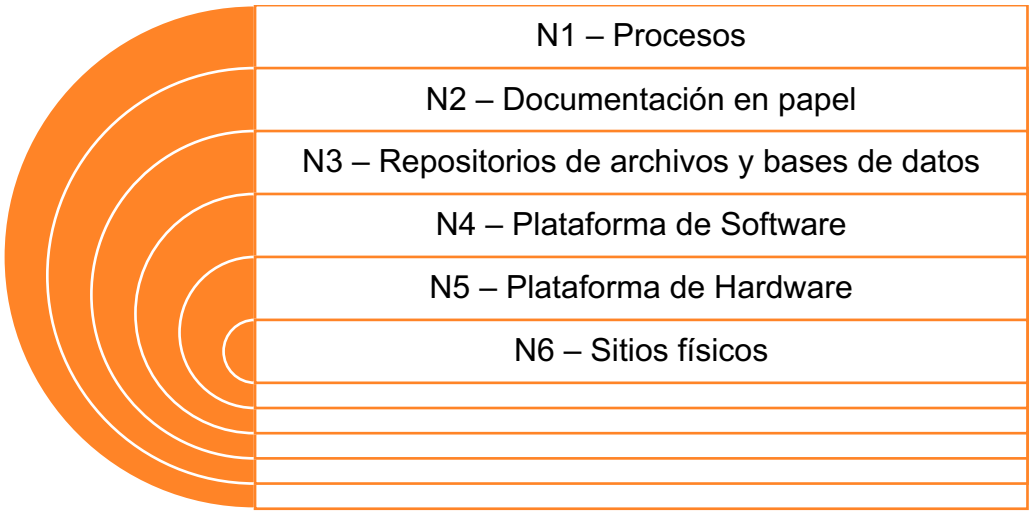
12.2.2. Interrelación de los activos de información

Como se identificó precedentemente, existen diferentes elementos que forman el universo de los activos de información; por lo cual resulta fundamental establecer la dependencia y relación entre ellos.

En una primera etapa se reconocen los procesos y procedimientos que lo componen. Luego se identifican y se vinculan la documentación en papel, repositorios de datos, aplicaciones, módulos y herramientas informáticas utilizadas

para cada uno de los procesos, la infraestructura tecnológica y los sitios físicos; y por último, los que no se encuentran en custodia de la entidad como proveedores y recursos humanos.

ESQUEMA N°63: Elementos de los sistemas contables en custodia de la entidad



Fuente: Elaboración propia.

Considerando esta dependencia, se puede identificar cómo repercute la infraestructura de las Tecnologías de Información a los procesos de la entidad, contribuyendo en:

- Establecer controles y procedimientos nuevos.
- Mejorar la calidad de la auditoría financiera.
- Incrementar la eficacia y eficiencia de las operaciones.
- Mejorar la administración de TI.

A continuación, se establecen las normas básicas a considerar para los diferentes activos de información en custodia de las entidades bancarias:

12.2.3. Estándares asociados a los activos de información N1 (Procesos) y N2 (Documentación en papel)

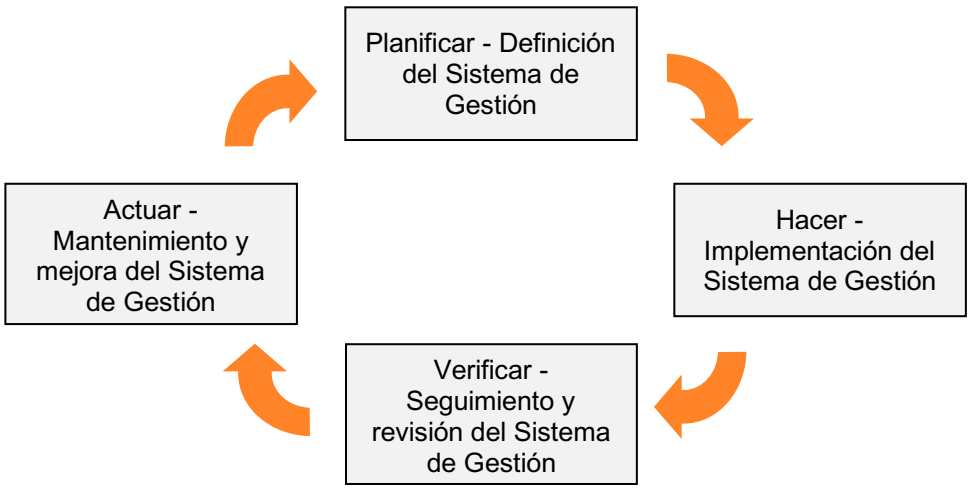
En esta sección se identificarán normas para analizar los procesos administrativos, de tecnología y de control interno.

12.2.3.1. Análisis de la calidad de los procesos administrativos (N1)

La IRAM/ISO 9001 plantea los requisitos para implantar un Sistema de Gestión de la Calidad, que puede utilizarse para su aplicación interna por las organizaciones; brindando la posibilidad de certificar la calidad de los procesos.

Todo sistema de gestión debe tener como base el modelo que es denominado “P-H-V-A” que involucra a los siguientes principios básicos: Planificar, Hacer, Verificar y Actuar. Los mismos deben ser considerados para contribuir con la mejora continua en todo proceso. En el siguiente esquema se identifican los mismos:

ESQUEMA N°64: Principios básicos de un sistema de gestión (P-H-V-A)



Fuente: (International Organization for Standardization, 2015)

Cada uno de los principios incluye las siguientes características:

ESQUEMA N°65: Tabla de principios básicos de la IRAM/ISO 9.001

Detalle de los principios básicos de la IRAM/ISO 9.001
Planificar: se relaciona con el establecimiento de políticas, objetivos, procesos y procedimientos con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Hacer: se relaciona con la implementación y gestión de la política, los controles, procesos y procedimientos del sistema.
Verificar: significa medir el desempeño del proceso contra la política y los objetivos planteados y reportar los resultados a la dirección, para su revisión.
Actuar: implica emprender acciones preventivas o correctivas teniendo en cuenta los resultados de la auditoría, sistema de gestión, la revisión por la dirección, u otra información relevante, para lograr la mejora continua.
Fuente: **(International Organization for Standardization, 2015)**

Esta norma, contribuye a organizar y a sistematizar los activos de información N1 ya que:

- Contiene los requisitos generales y los específicos para gestionar la documentación empresaria.
- Establecen requisitos que debe cumplir la dirección de la organización, tales como definir la política, asegurar que las responsabilidades y autoridades estén definidas, aprobar objetivos, etc.
- Análisis y mejora continua de los procesos y procedimientos.
- Permiten la implantación de otras normas ISO.

12.2.3.2. Análisis de la estructura del control interno organizacional

En el campo del ejercicio profesional existe un marco de referencia denominado "Informe COSO" (Committee of Sponsoring Organizations of the Tread, 2013), en el cual se define al control interno, como:

> *"un proceso efectuado por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de los objetivos dentro de las siguientes categorías:*
>
> - *Eficacia y eficiencia de las operaciones.*
> - *Confiabilidad de la información financiera.*
> - *Cumplimiento de las leyes, reglamentos y normas*" (Instituto de Auditores Internos de Argentina, 2019)

En el siguiente esquema se identifican los elementos que deben implementarse en la estructura de control interno en las organizaciones:

ESQUEMA N°66: Informe COSO 2

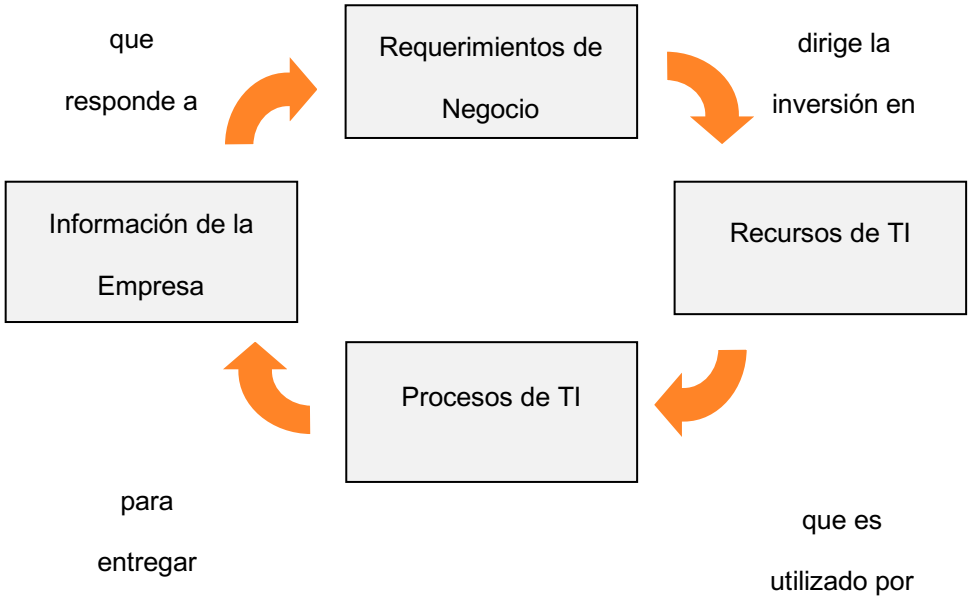
Fuente: Informe COSO II. (Committee of Sponsoring Organizations of the Tread, 2013)

12.2.4. Estándares asociados a los activos de información N3 (Repositorios de archivos y bases de datos), N4 (Plataforma de Software) y N5 (Plataforma de Hardware).

12.2.4.1. Para gestionar los procesos de TI

El marco COBIT: Objetivos de Control para Información y Tecnologías Relacionadas (Instituto de Auditores Internos de Argentina, 2019), es un estándar de trabajo de Gobierno de Tecnología de Información (TI) que permite a la gerencia cerrar la brecha entre los requerimientos de control, aspectos técnicos y riesgos de negocios. Este marco habilita el desarrollo de políticas claras y buenas prácticas para el control de TI en todas las áreas de la organización.

ESQUEMA N°67: Principios básicos de COBIT



Fuente: (Information Systems Audit and Control Association, 2019)

12.2.4.2. Para el análisis de las transacciones de la tarjeta de pago

Las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial.

Las PCI DSS constituyen un conjunto mínimo de requisitos para proteger datos de titulares de tarjetas y se pueden mejorar con el uso de controles y prácticas adicionales para mitigar otros riesgos.

12.2.4.3. ITIL

El Marco Normativo ITIL (Information Technology Infrastructure Library) o en español, “Biblioteca de Infraestructura de Tecnologías de Información” presenta buenas prácticas utilizadas en la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general.

12.2.5. Estándares asociados a todos los activos de información

12.2.5.1. IRAM/ISO/IEC 27.001

El Sistema de Gestión de Seguridad de la Información es definido como un “Proceso sistemático, documentado y conocido por toda la organización. Y basado

en un enfoque por riesgo de negocio, el SGSI es un modelo para el establecimiento, implementación, operación, control, revisión, mantenimiento y mejora de la seguridad de la información." (IRAM/ISO/IEC, 2018)

Enfocado en este concepto, la norma IRAM/ISO/IEC 27.001 brinda un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un SGSI. La misma establece los siguientes 11 dominios a tener en cuenta para implantar en la Gestión de la Seguridad:

ESQUEMA N°68: Tabla de Dominios de la IRAM/ISO/IEC 27.001

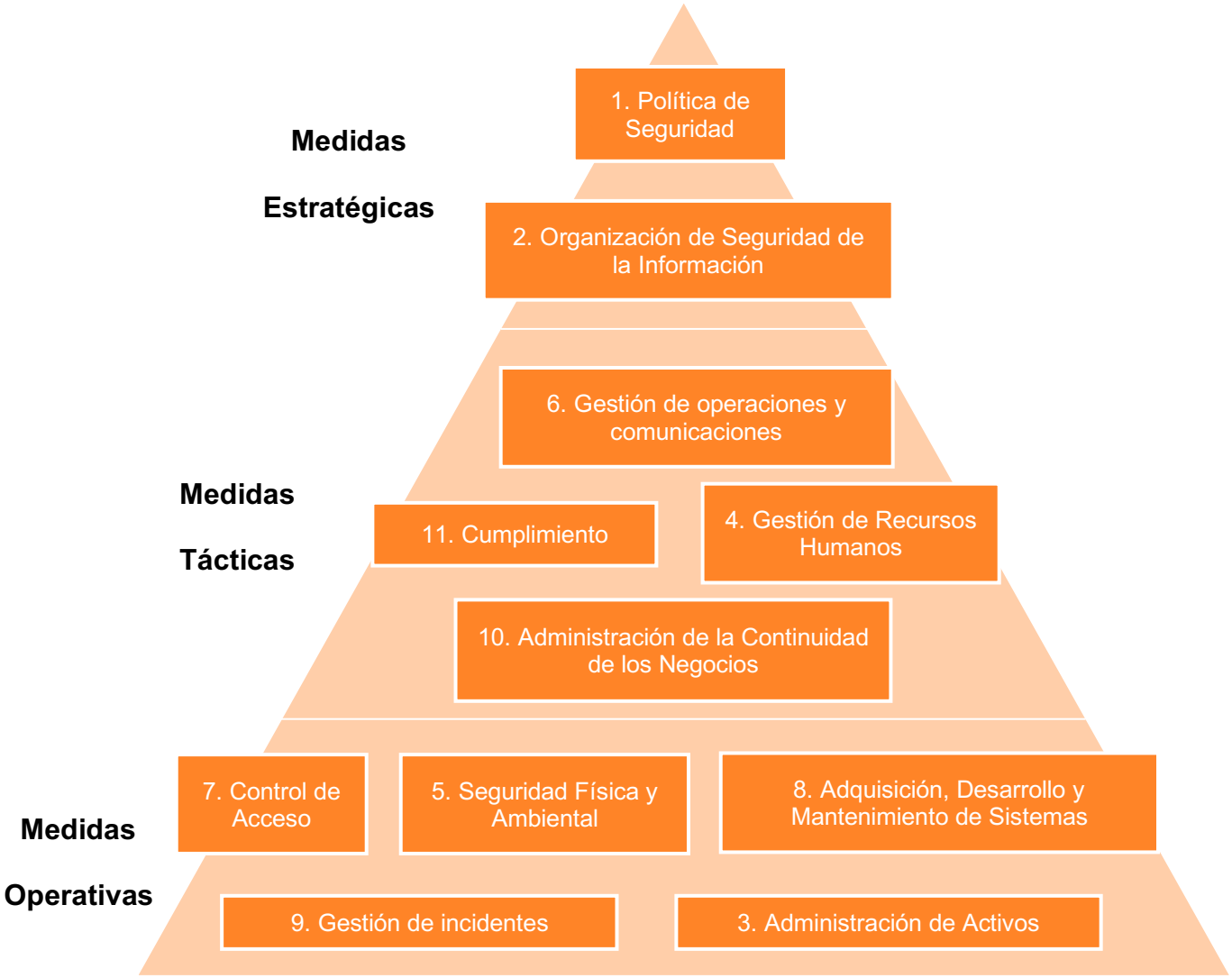
Dominios de la IRAM/ISO/IEC 27.001	
Aspectos cubiertos por la norma IRAM/ISO/IEC 27.001	1. Política de Seguridad.
	2. Organización de Seguridad de la Información.
	3. Administración de Activos.
	4. Gestión de Recursos Humanos.
	5. Seguridad Física y Ambiental.
	6. Gestión de operaciones y comunicaciones.
	7. Control de Acceso.
	8. Adquisición, Desarrollo y Mantenimiento de sistemas.
	9. Gestión de incidentes.
	10. Administración de la Continuidad de los Negocios.
	11. Cumplimiento de la normativa Legal Vigente.
Fuente: (IRAM/ISO/IEC, 2018)	

Se destaca que cada uno de los aspectos cubiertos corresponde a características en los sistemas de gestión de la seguridad que no se encuentran exclusivamente

relacionados con términos tecnológicos, ya que en la administración de la seguridad se necesita redactar políticas estratégicas, normas, procedimientos y establecer controles a los procesos en las entidades.

Teniendo en cuenta estos principios, se los pueden relacionar con las diferentes decisiones y funciones tomadas en los niveles de la organización, en los cuales se pueden subdividir en decisiones estratégicas, tácticas y operativas.

ESQUEMA N°69: Niveles organizacionales y los dominios establecidos por la IRAM/ISO/IEC 27.001

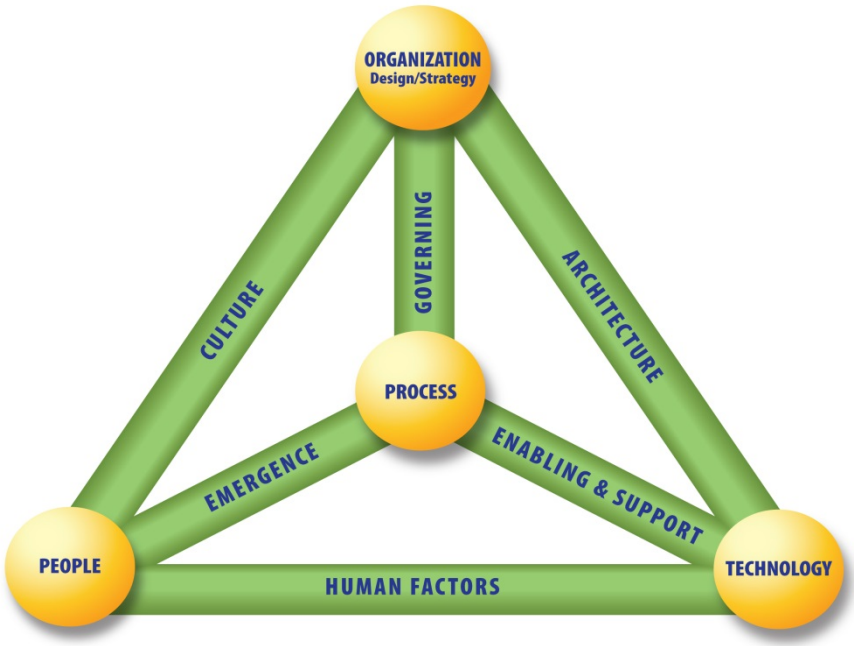


Fuente: (IRAM/ISO/IEC, 2018)

12.2.5.2. Modelo de Gestión de la Seguridad Informática

El Modelo de Negocio de Seguridad Informática o "The Business Model for Information Security" (BMIS) fue desarrollado y difundido por la asociación ISACA. La principal característica de este modelo radica en el establecimiento como ejes fundamentales en la gestión de la seguridad a las personas, procesos, tecnologías y organización del ente:

ESQUEMA N°70: Modelo de Negocio de Seguridad Informática



Fuente: "The Business Model for Information Security" (ISACA, 2010)

Al analizar el mismo se puede destacar el rol que se le da a la cultura, ya que se establece como una de las aristas del modelo ya que define la relación entre la

organización de la entidad y a las personas, pero este marco solo tiene en cuenta a las personas involucradas internamente en la organización, y no contemplando a las externas.

12.2.5.3. Information Security Management Maturity Model (ISM3)

El modelo de ISM3 (Information Security Management Maturity Model), ofrece un nuevo enfoque de los sistemas de gestión de seguridad de la información orientado exclusivamente a los sistemas de gestión de calidad, ISO 9.001 en las organizaciones.

Si bien es un modelo novedoso, no se orienta exclusivamente en la capacitación, pero como establece (Vicente, 2019), el modelo "*ISM3 proporciona un que puede utilizarse tanto por pequeñas organizaciones que realizan sus primeros esfuerzos, como a un nivel alto de sofisticación por grandes organizaciones como parte de sus procesos de seguridad de la información.*"

12.2.5.4. Information Security Forum's Standard of Good Practice (SOGP).

El modelo SOGP "Information Security Forum's Standard of Good Practice" es un marco con buenas prácticas basado en las experiencias del ISF (El Foro de Seguridad de la Información). Este estándar es una guía para la seguridad de la información enfocada exclusivamente en el negocio, la cual se organiza en cuatro categorías principales:

- Gobierno de la seguridad
- Requisitos de seguridad
- Marco de control
- Seguimiento y mejora de la seguridad

En el Foro de Seguridad de la Información (2010), se describe que este "*estándar cubre temas como la estrategia de seguridad, la gestión de incidentes, la continuidad del negocio, la capacidad de recuperación y la gestión de crisis*", pero se basa en consejos prácticos para mejorar la capacidad de resistencia de la organización frente a una amplia gama de amenazas y eventos que pueden amenazar el éxito e incluso la supervivencia de la organización.

12.2.5.5. Otras normas

Existen otros modelos que analizan indirectamente cuestiones de seguridad. Uno de ellos es el caso de ITIL que tiene muchos puntos de contacto respecto a cuestiones de seguridad. Otra es la norma Prince2, que se orienta en la seguridad relacionada con la gestión de proyectos; también se puede destacar el modelo TLLJO, que se enfoca la implementación de un SGSI, permitiendo un mayor control sobre el sistema a un precio moderadamente reducido.

En el ámbito internacional, el NIST (National Institute of Standards and Technology) que cuenta con una división especializada en seguridad de la información ha publicado la norma SP 800-30 del NIST, la que ha influido en la mayoría de las

normativas sobre análisis de los riesgos de los activos. Otra metodología muy utilizada es OCTAVE, publicada por el CERT (Coordination Center de la Universidad de Carnegie Mellon); que *"cuenta con una versión para pequeñas y medianas empresas conocida como OCTAVE-S"* (Portantier F. , 2019).

12.3. Control de los activos de información en custodia de proveedores

12.3.1. Introducción

En la actualidad las entidades bancarias tienen la posibilidad de contratar servicios tercerizados para el manejo de la información. Estos servicios pueden ser clasificados en proveedores que manejan datos bajo una infraestructura tecnológica; proveedores que brindan otros tipos de servicios no tecnológicos, pero manejan información y aquellos que no manejan datos.

Dentro de los tecnológicos, se pueden identificar los que ofrecen sistemas de información en la "*nube*" con la posibilidad de contar con soluciones de software escalable y disponible las 24 horas para procesar datos corporativos.

En el presente capítulo se analizarán los conceptos básicos de computación en la Nube, sus implicancias legales y lo que establece el BCRA para el cuidado de este tipo de activo de información en entidades bancarias.

12.3.2. Clasificación de servicios tercerizados según el BCRA

En el tratamiento de información en custodia de terceras partes, el BCRA en la Comunicación “A” 6354 (2017) clasificó los siguientes servicios brindados por el proveedor que manejan datos como “Servicios de Tecnología Informática” (STI). Los mismos comprenden:

> *“a la prestación formal, regular, periódica, delimitada y controlada de recursos de tecnología informática indispensables para brindar alguno o varios de los siguientes servicios: infraestructura informática, procesamiento de datos, operaciones y mantenimiento, comunicaciones, almacenamiento y custodia, desarrollo de aplicaciones y contingencia; siempre que los mismos tengan un impacto directo o indirecto sobre datos del cliente, datos contables-financieros o datos transaccionales.”* Comunicación “A” 6354 del BCRA (2017)

ESQUEMA N°71: Tipos de servicios de tecnología informática que manejan datos

Infraestructura de Tecnología y Sistemas (SIS)

- Comprende a todos los recursos informáticos, operativos y de información dispuestos para la administración, operación, desarrollo, mantenimiento, procesamiento y control de los STI.

Procesamiento de Datos (SPD)

- Comprende todos los recursos humanos, informáticos y operativos dispuestos para la operación, ingreso, transformación y salida de datos mediante el uso de funciones, instrucciones o aplicaciones programadas de manera controlada y repetitiva, integrados a un STI.

Soporte, Prevención y Mantenimiento (SPM)

- Comprende todos los recursos humanos, informáticos y operativos dispuestos para brindar soporte, mantenimiento, técnicas de prevención y/o análisis de datos de los STI.

Comunicaciones (STC)

- Abarca a todos los recursos informáticos y operativos dispuestos para la administración, operación, disponibilidad, mantenimiento y transporte de voz, datos, imagen o video que se interconectan e integran a los recursos de la infraestructura de tecnología y sistemas (SIS) de un STI.

Almacenamiento y Custodia (SAC)

- Comprende todos los recursos informáticos, operativos y de información dispuestos para el registro, conservación, recupero y explotación de datos integrados a un STI.

Desarrollo de Aplicaciones (SDA)

- Abarca a todos los recursos humanos y de software, metodología, licencias, diseño, conocimiento, mano de obra, prueba y mantenimiento para la programación/adquisición de piezas de software aplicativo o rutinas programadas para el uso/explotación de datos productivos.

Contingencia y Recuperación (SCR)

- Comprende a todos los recursos informáticos y operativos dispuestos para la administración, operación y mantenimiento de los procesos de continuidad operativa, recuperación de datos, procesamiento alternativo, soporte técnico y logístico en contingencia, de acuerdo con la demanda establecida para cada STI.

Fuente: Comunicación “A” 6354 del BCRA (2017)

De los mencionados el más crítico es el servicio de procesamiento de datos, para poder identificar las posibilidades existentes se analizará a continuación el concepto de computación en la nube.

12.3.3. Cuestiones básicas del servicio de "computación en la nube"

La contratación de soluciones de "Computación en la nube" es descripta como una forma de prestación de servicios para el tratamiento de la información, depositando en la infraestructura tecnológica de un tercero los datos para el procesamiento de los mismos.

Actualmente se ofrece como una gran ventaja a las entidades ya que no tiene necesidad de realizar inversiones en infraestructura de software y hardware, con la posibilidad de acceder a los servicios a través de internet. Y en este caso *"El proveedor puede encontrarse, prácticamente, en cualquier lugar del mundo y su objetivo último será proporcionar los servicios citados optimizando sus propios recursos a través de, por ejemplo, prácticas de deslocalización, compartición de recursos y movilidad o realizando subcontrataciones adicionales"* (Agencia Española de Protección de Datos, 2017). Pero dentro de las definiciones de "computación en la nube" encontramos 3 modelos diferentes:

ESQUEMA N°72: Modelos de Computación en la Nube

Fuente: Elaboración Propia.

- ***NUBE PÚBLICA***

Se considera un servicio de nube pública cuando "*el proveedor de servicios de cloud proporciona sus recursos de forma abierta a entidades heterogéneas, sin más relación entre sí que haber cerrado un contrato con el mismo proveedor de servicio*".[2]

- ***NUBE PRIVADA***

Un servicio de nube es considerado privado cuando un ente realiza la gestión y administración de sus servicios en la nube para las partes que la forman, sin que en la misma puedan participar entidades externas y manteniendo el control sobre ella. "*Una Nube Privada no necesariamente se implementa por la misma entidad que la utiliza, sino que puede contratarse a un tercero que actuará bajo su supervisión y en función de sus necesidades.*"[2]

- ***NUBE HÍBRIDA***

Se considera un servicio de nube híbrida cuando existen determinados servicios que se ofrecen de forma pública y otros de forma privada.

Independientemente de los modelos expuestos, que dependerá de la envergadura del ente y el tipo de información analizada, pueden contratar diferentes modalidades de servicio. A continuación, se analizan los más importantes:

ESQUEMA N°73: Tipos de servicios de computación en la nube

Fuente: Elaboración Propia.

- ***Software como servicio "Software as a Service o SaaS".***

En este tipo de servicio el usuario encuentra en la nube las herramientas finales con las que *"puede implementar directamente los procesos de su empresa: una aplicación de contabilidad, de correo electrónico, un worlkflow, un programa para la gestión documental de su empresa, etc."*

- ***Plataforma como servicio "Platform as a Service o PaaS".***

En este servicio se proporcionan utilidades para construir aplicaciones, un sistema operativo instalado y una base de datos. Por lo tanto, se pueden construir, instalar y ejecutar aplicaciones.

- ***Infraestructura como servicio "Infraestructure as a Service o IaaS".***

En este tipo de servicio, el proveedor proporciona capacidades de almacenamiento y proceso en bruto, *"sobre las que el usuario ha de construir las aplicaciones que necesita su empresa prácticamente desde cero",* en este caso las empresas pueden establecer sus plataformas, aplicativos y bases de datos.

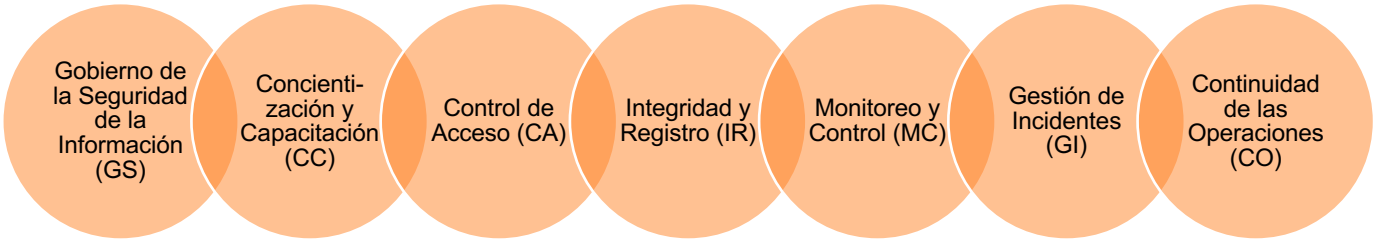
Dados estos conceptos básicos, se puede identificar todas las posibilidades de servicios de procesamiento de datos. Cuando una organización decide contratar este tipo de servicio para la entidad, debe considerar qué tipo de modelo y servicio se está adquiriendo para analizar correctamente los riesgos y la dependencia sobre este proveedor.

12.3.4. Tratamiento de los activos de información en custodia de terceras partes según lo dispuesto por el BCRA

En el caso de "Servicios de Tecnología Informática" brindado por los proveedores, el BCRA establece que las entidades financieras y proveedores *"deben poseer la funcionalidad y propósito descriptos en los procesos de seguridad"* e informar al organismo de control *"la estructura e interrelaciones orgánicas y operativas que en*

sus organizaciones se corresponda". En siguiente esquema se identifican los procesos de estructura y organización en la gestión de los servicios tercerizados:

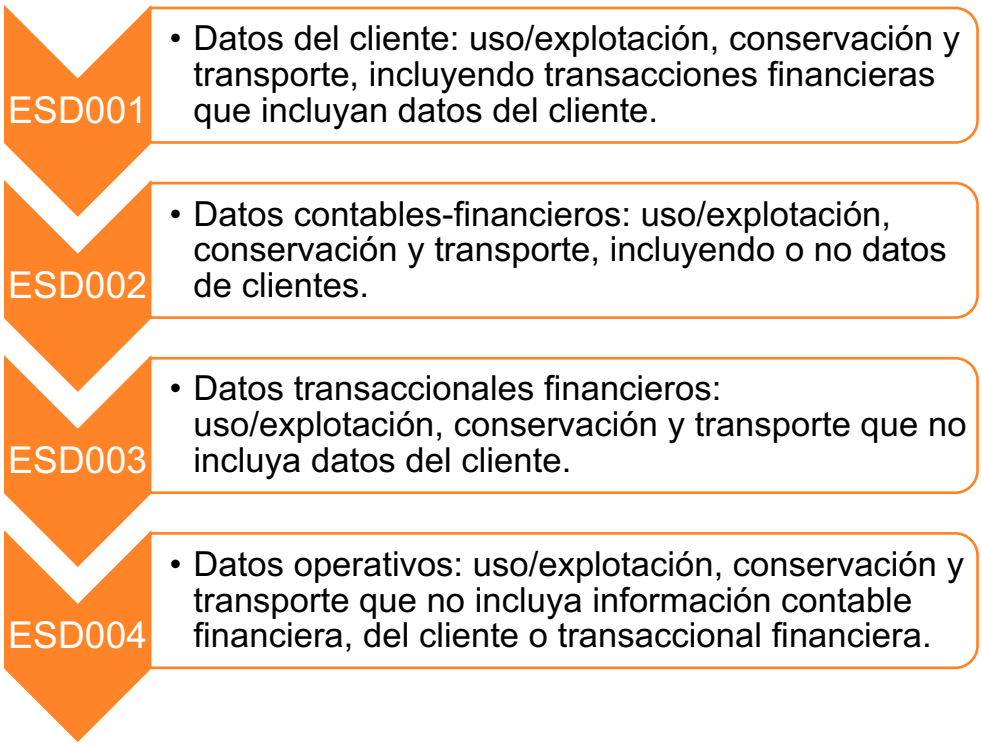
ESQUEMA N°74: Estructura y organizaciones identificadas en la Comunicación "A" 6354



Fuente: Comunicación "A" 6354 del BCRA (2017)

En esta línea, el BCRA estableció los tipos de datos en relación con los servicios brindados. Se puede identificar datos del Cliente, Contable-Financieros, transaccionales financieros y los operativos; en el siguiente esquema son descriptos según lo establecido por el organismo de control:

ESQUEMA N°75: Tipos de datos



Fuente: Comunicación “A” 6354 del BCRA (2017)

Para poder analizar la criticidad de cada uno de los servicios tercerizados es necesario que las entidades establezcan una metodología para analizar a los proveedores teniendo en cuenta al tipo de dato en custodia y el tipo de servicio brindado por la empresa.

Asimismo, el BCRA establece que las entidades bancarias deberán implementar *"un entorno no operativo que permita ejercer el control activo, continuo y permanente de todas las actividades indicadas en el acuerdo de STI tercerizado y los datos".* El citado entorno es denominado: Punto de Acceso Unificado; con el objetivo de poder controlar la disponibilidad y todos los aspectos que la entidad considere pertinente.

En el marco de la presente investigación se desarrolló un modelo de selección de proveedores utilizando metodologías borrosas que se complementa con lo dispuesto por el BCRA; dicha metodología se encuentra en el Anexo I de la presente tesis.

12.4. Control de la información conocida por los recursos humanos: Identificación de mejores prácticas y estándares de capacitación y concientización

12.4.1. Introducción

En las entidades bancarias, la información analizada, procesada y en conocimiento del personal existente para ser cuidada y protegida debe basarse principalmente en la capacitación y concientización.

Para ello resulta fundamental establecer un plan de capacitación adecuado a las necesidades de los Recursos Humanos y de todas aquellas personas que manejen información bancaria, como es el caso de clientes y proveedores.

El presente capítulo tiene el objetivo de analizar teóricamente los conceptos principales relacionados con la educación, cultura informativa, modelos de gestión y modelos de madurez cultural para el cuidado de los activos de la información.

12.4.2. Capacitación en seguridad de la información

Hace más de dos décadas que el National Institute of Standards and Technology (NIST) viene desarrollando diferentes manuales estableciendo diferencias a tener en cuenta en la gestión y en los planes de acción en el cuidado de la información. En la planificación de los programas de capacitación en Seguridad de la Información, resulta fundamental, distinguir las características y las diferencias entre concientización, formación y educación. En el manual "An Introduction to Computer Security", el NIST (2019) estableció las citadas diferencias.

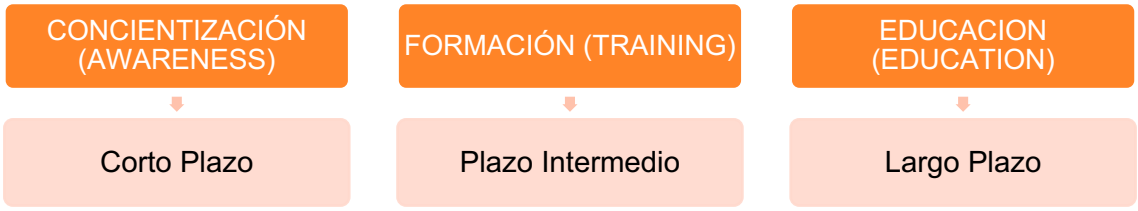
ESQUEMA N°76: Concientización, formación y educación

Fuente: (National Institute of Standards and Technology, 2019)

En primer lugar, establece que en las organizaciones la concientización está relacionada al nivel *informativo de la capacitación*, a diferencia de la formación, que se encuentra basada en el conocimiento, y la Educación, con la percepción y la capacidad de interpretar los conocimientos.

Teniendo en cuenta a las características inherentes, podemos establecer el plazo necesario para cumplir los objetivos que se necesita para la implementación y el dictado de cada una:

ESQUEMA N°77: Planificación de Concientización, Formación y Educación



Fuente: (National Institute of Standards and Technology, 2019)

De lo indicado en el esquema anterior, es importante destacar que los planes de concientización son a corto plazo y con alto impacto, ya que está relacionada al nivel informativo de la capacitación. Para una mejor comprensión, se expone textualmente y a fines informativos el cuadro comparativo desarrollado y publicado por el NIST:

ESQUEMA N°78: Diferencia entre capacitación, entrenamiento y educación

	CAPACITACIÓN	ENTRENAMIENTO	EDUCACION
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Teaching Method:	Media - Video - Newsletters - Posters, etc.	Practical Instruction - Lecture - Case study workshop - Hands-on practice	Theoretical Instruction - Discussion seminar - Background reading
Test Measure:	True/False Multiple Choice (identify learning)	Problem Solving (applylearning)	Eassay (interpretlearning)
Impact Timeframe:	Short-term	Intermediate	Long-term

Fuente: Compares some of the differences in awareness, training, and education. (National Institute of Standards and Technology, 2019)

Teniendo en cuenta los objetivos planteados en este capítulo, se remarca el corto plazo y alto impacto, como una característica de los planes de concientización, ya

que está relacionada al nivel informativo de la capacitación al desarrollar un programa de concientización.

Asimismo, analizando las herramientas y medios de comunicación disponibles para la concientización, se encuentran centrados en videos, boletines de información o carteles, entre otros, con actividades o métodos de difusión con alto impacto. Y con relación a las medidas de pruebas para identificar el aprendizaje propuesto, se recomiendan realizar preguntas mediante la metodología de selección múltiple o respuestas del tipo verdadero -falso.

12.4.3. La cultura informativa

Como se indicó en la introducción, el nivel de la seguridad y concientización de la información en entidades bancarias se encuentra relacionado con la cultura informativa de las organizaciones.

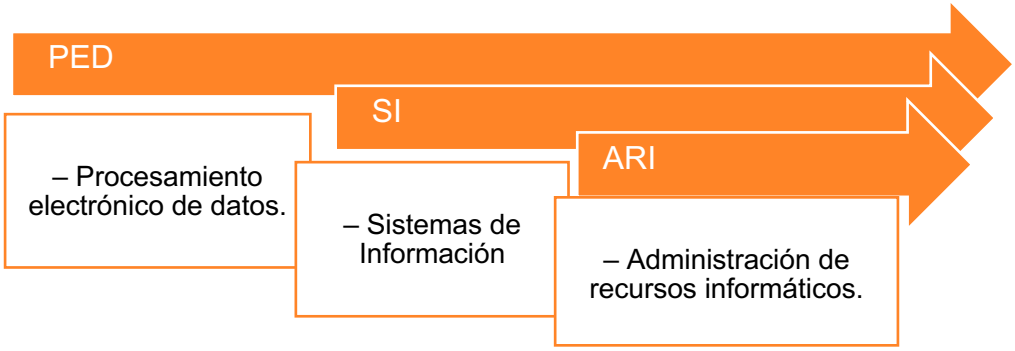
En el modelo de "estado de la Cultura Informativa", (Tesoro, 1998) identifica tres tipos de niveles culturales relacionados con la forma en que las organizaciones usan los recursos de IT. Los mismos pueden ser clasificados como operativo, integrador o estratégico de la tecnología.

ESQUEMA N°79: Nivel de la cultura informativa

Fuente: (Tesoro, 1998)

Cada uno de los niveles, tiene características específicas que fue desarrollado por (Saroka, 2020), en donde manifiesta que organizaciones pueden tener los siguientes enfoques:

ESQUEMA N°80: Estructura de tecnología existente



Fuente: Elaboración Propia basado en (Saroka, 2020)

En una organización con un nivel operativo de cultura informativa, el ambiente de utilización de los recursos informáticos es únicamente de procesamiento electrónico de datos (PED), con un enfoque para el planeamiento de recursos orientado en cuestiones técnicas y operativas:

- Planeamiento por el vendedor del equipo.
- Planeamiento por estudios especiales
- Planeamiento por técnicos.

Si una organización tuviera un nivel integrador de cultura informativa, el ambiente de utilización de los recursos informáticos es el de sistemas de información (SI), que utiliza un enfoque para el planeamiento de recursos enfocados a los sistemas implementados.

Y en el caso de una organización con un nivel estratégico de cultura informativa, el ambiente de utilización está orientado a la administración de recursos informáticos (ARI) con un enfoque de planeamiento de recursos asociado al planeamiento estratégico, tratando de alinear el uso de las tecnologías a las estrategias principales de la organización.

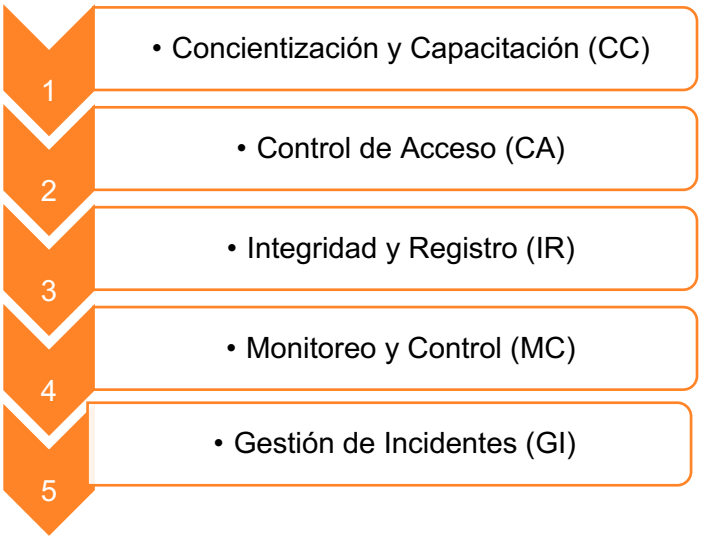
Estos niveles tienen que ser tenidos en cuenta al analizar el grado de madurez de la seguridad y el modelo de gestión a implementar.

12.4.4. Los canales electrónicos en las entidades bancarias

En el año 2016, entró en vigencia la Comunicación “A” 6017 del (BCRA) la cuál modificó la Comunicación “A” 5374 del (BCRA, 2012) estableciendo nuevos requisitos y medidas a implementar en los Canales Electrónicos en donde operan los clientes de las entidades bancarias.

La citada norma de cumplimiento obligatorio incluye a la “Concientización y capacitación” de los empleados, clientes y proveedores dentro de los procesos específicos de los mencionados canales:

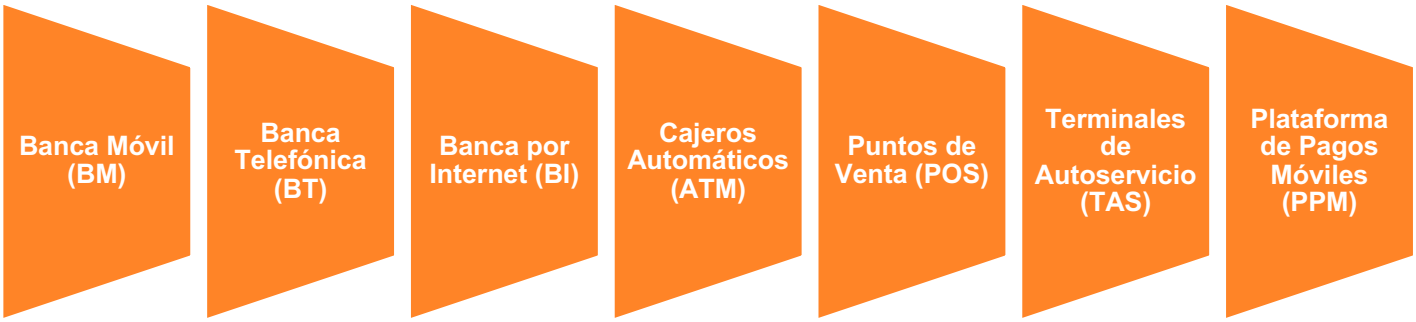
ESQUEMA N°81: Procesos establecidos en la Comunicación "A" 6017 del BCRA



Fuente: Elaboración Propia basado en (BCRA, 2016)

Para cada uno de estos, el BCRA especifica los criterios y los procedimientos a implementar por la entidad; planteando un nuevo desafío en la gestión de la Seguridad en las entidades bancarias. La citada Comunicación establece que "*se encuentran alcanzadas las entidades financieras que intervengan en la prestación, por sí o por terceros en su nombre, de servicios financieros por intermedio de algunos de los siguientes Canales Electrónicos (CE)"* (BCRA, 2016).

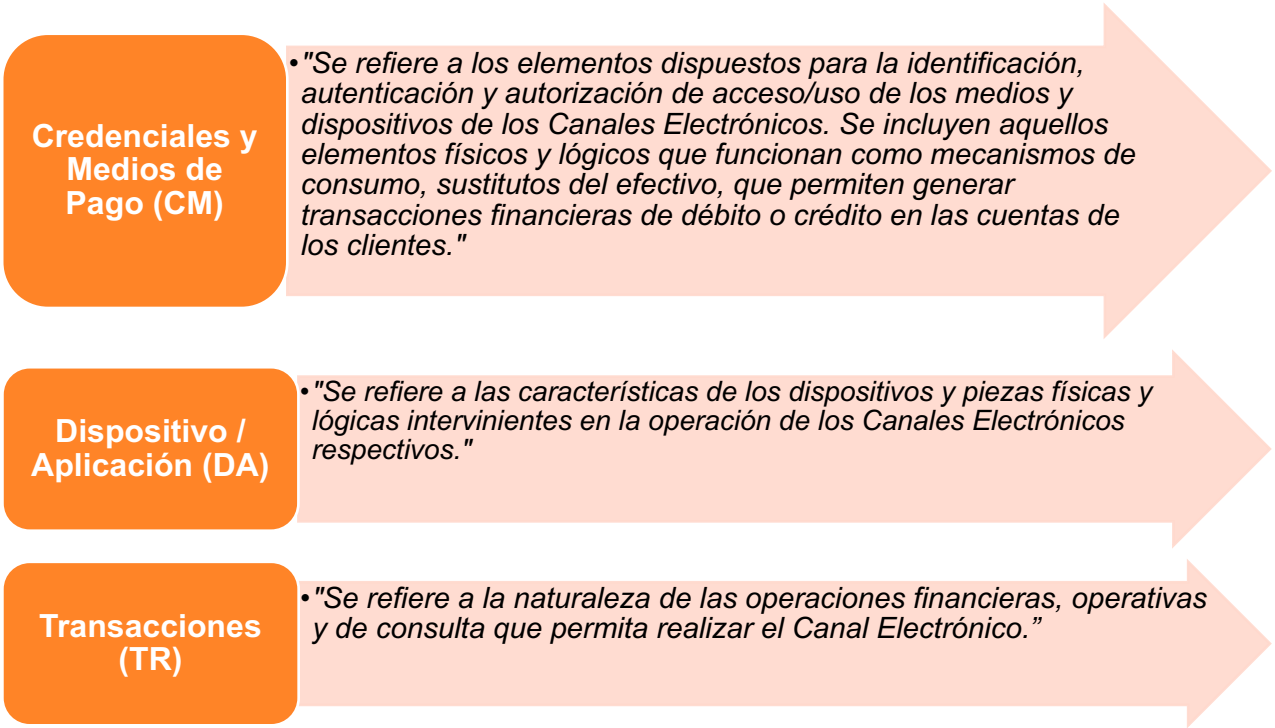
ESQUEMA N°82: Canales Electrónicos



Fuente: Elaboración Propia basado en (BCRA, 2016)

Además, para el análisis de cada canal se establecen los “escenarios”, que están representados en tres categorías y agrupados por el mismo interés:

ESQUEMA N°83: Escenarios en Canales Electrónicos



Fuente: Elaboración Propia basado en (BCRA, 2016)

Teniendo en cuenta los escenarios y los canales electrónicos, resulta fundamental describir en primer lugar a los destinatarios de la concientización y capacitación dispuesta por la normativa vigente. Con ese fin, se identifica al “Cliente Externo”, con los clientes que operan por los canales electrónicos y al “Cliente Interno” con los empleados de la entidad.

Considerando todo lo expuesto, a continuación, se presentan los requisitos mínimos de Concientización y Capacitación que es exigida por la norma:

ESQUEMA N°84: Requisitos mínimos de Concientización y Capacitación

Código de requisito	Descripción de requisito
RCC001	Los contenidos del programa de CC deben formularse y mantenerse actualizados en base a un análisis de las vulnerabilidades y los resultados de la Gestión de Incidentes, e incluir, pero no limitarse a incidentes: reportados, detectados y conocidos.
RCC002	Los contenidos del programa de CC deben incluir: técnicas de detección y prevención de apropiación de datos personales y de las credenciales mediante ataques de tipo “ingeniería social”, “phishing”, “vishing” y otros de similares características.
RCC003	Los contenidos del programa de CC deben incluir: técnicas de detección y prevención del “skimming” y apropiación de datos de las credenciales mediante técnicas de intervención física.
RCC004	Los contenidos del programa de CC deben incluir: técnicas de detección de situaciones sospechosas en el recinto o entorno de acceso al CE.
RCC005	Mantener informado al personal interno, personal responsable por la gestión del CE, personal de terceros involucrado en las tareas operativas y clientes sobre las vías de comunicación para la recepción de denuncias o problemas en el circuito asociado al escenario descripto.
RCC006	Respecto de la audiencia del programa de CC, deben aplicarse los siguientes criterios: a. Características y segmentación de la audiencia, de acuerdo con el nivel de intervención en el proceso y naturaleza de la función o rol que ocupa cada participante. b. Deben encontrarse alcanzados todos los participantes necesarios en el flujo completo de la actividad indicada en el escenario. c. Orientado, pero no limitado a: personal interno, personal responsable por la gestión del CE, proveedores y clientes.

RCC007	Con una periodicidad mínima anual, debe efectuarse un análisis del Programa de CC ejecutado que mida la evolución de los incidentes, respecto de las actividades de CC realizadas incluyendo como mínimo: a. Un reporte de la cantidad y segmentación de destinatarios y contenidos del programa de CC. b. Una comparación entre los contenidos cubiertos por el programa de CC y la cantidad y tipo de incidentes de seguridad reportados/detectados/conocidos.
RCC008	Los contenidos del programa de CC deben incluir: medidas y técnicas para la protección de la privacidad de las credenciales.
RCC009	Los contenidos del programa de CC deben incluir: recomendaciones específicas sobre el uso seguro de los dispositivos propios del usuario y los dispositivos provistos por la entidad/operador.
RCC010	Los contenidos del programa de CC deben incluir: recomendaciones específicas sobre las prácticas de seguridad en la plataforma de soporte de CE.
RCC011	Los contenidos del programa de CC deben incluir: acciones específicas del usuario para la configuración de los dispositivos propios para comunicación con el CE (teléfonos, computadores personales, tabletas electrónicas, entre otros). Incluye, pero no se limita a las características diferenciadas por dispositivo para el almacenamiento de datos, reposo/bloqueo automático, eliminación de información antes del descarte o reemplazo del dispositivo, actualización de sistemas operativos y piezas de software provistas por la entidad para uso del CE.
RCC012	Los contenidos del programa de CC deben incluir técnicas específicas para el desarrollo/adquisición/fabricación, implementación, homologación y prueba de características de seguridad de los dispositivos y piezas de software provisto por la entidad/operador, asegurando que el personal involucrado interno/externo se encuentra debidamente capacitado para disminuir las fallas de implementación de las características de seguridad.
RCC013	Las entidades/operadores deben contar con un mecanismo de comunicación de los contenidos de su programa de concientización y capacitación que asegure:

	a. Que los destinatarios se encuentran continuamente informados. b. Que los destinatarios pueden efectuar consultas y evacuar dudas.
RCC014	En la selección/cambio, por parte del cliente, de los valores de los elementos de autenticación basados en el factor "algo que sabe", la entidad/operador deben recomendar al titular que los valores no se compongan al menos de: a. Una secuencia de número asociado a un dato personal público. b. Serie de caracteres o números iguales. c. Incremento o decremento de número consecutivo. d. Fechas de significación histórica.

Fuente: Comunicación "A" 6017 (BCRA, 2016)

A continuación, se expondrán los modelos para gestionar la capacitación y concientización al personal sobre los activos de información existentes en entidades bancarias.

12.4.5. Modelos de madurez cultural de la Seguridad de la Información

Actualmente existen muchos modelos relacionados con la madurez cultural de la organización. En la presente sección se presentan los modelos más relevantes teniendo en cuenta la madurez de la cultura en la Seguridad de la Información.

12.4.5.1. Modelo de Evaluación de la Seguridad de la Información de Citigroup (CITII-SEM)

Este modelo se centra en la concienciación y adaptación por parte de la organización en seguridad, el mismo es denominado “Modelo de Evaluación de la Seguridad de la Información de Citigroup”. En el siguiente esquema pueden observarse los posibles niveles de concientización en las entidades:

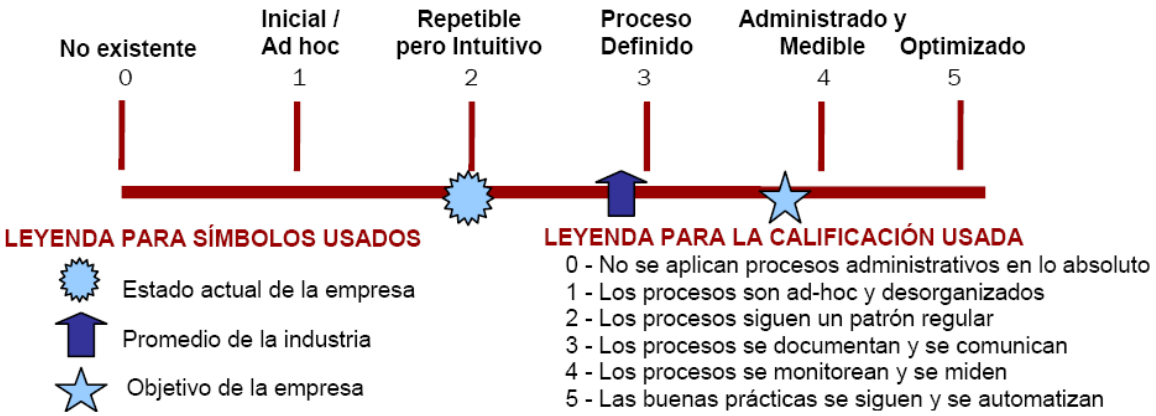
ESQUEMA N°85: Modelo de Evaluación de la Seguridad de la Información de Citigroup

Fuente: Basado en (CitiGroup, 2018)

12.4.5.2. Modelo de madurez de COBIT

Este popular modelo se centra en los procedimientos específicos de auditoría, lo que permitiría complementarlo con otras normas y actividades de control. Presenta seis niveles de madurez progresiva, comenzando por “no existente” hasta “optimizado”. En el siguiente esquema pueden observarse los niveles que serían alcanzables por las entidades:

ESQUEMA N°86: Modelo de Madurez COBIT

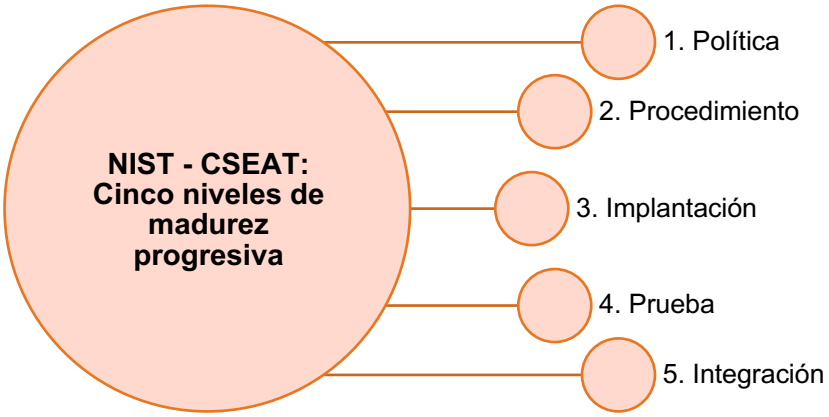


Fuente: COBIT 5. (Information Systems Audit and Control Association, 2019)

12.4.5.3. Modelo de Madurez de Seguridad en TI del NIST-CSEAT

Este modelo difundido por el NIST – CSEAT, presenta cinco niveles de madurez progresiva, orientada a los niveles de documentación en la organización. En el siguiente esquema pueden observarse los posibles niveles de madurez en las entidades:

ESQUEMA N°87: Centrado en niveles de documentación



Fuente: (National Institute of Standards and Technology, 2019)

12.4.5.4. Modelo de Madurez Capacidad de Ingeniería en Seguridad de los Sistemas (SSE-CMM)

Este modelo de madurez, denominado Modelo de Madurez Capacidad de Ingeniería en Seguridad de los Sistemas - SSE-CMM - (The International Systems Security Engineering Association (ISSEA), 2019), se basa en la madurez en la ingeniería de seguridad y diseño de software. En el siguiente esquema, se detallan los 5 niveles:

ESQUEMA N°88: Modelo SSE-CMM

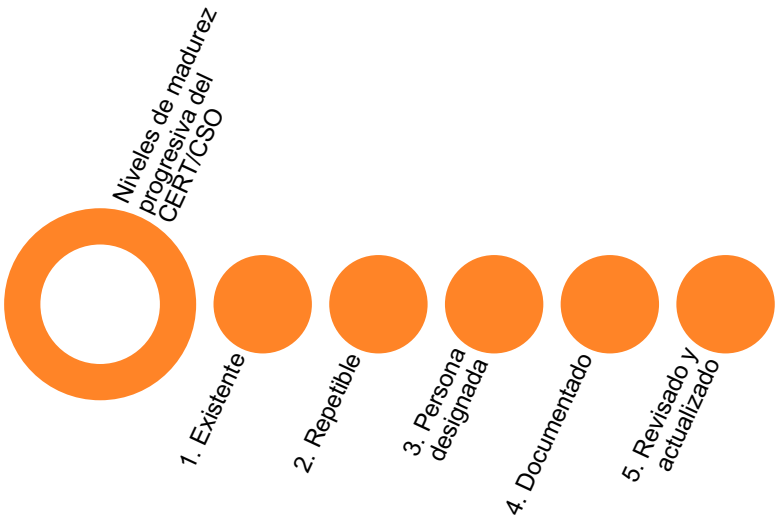
SSE-CMM: Cinco niveles de madurez progresiva	1. Realizado informalmente
	2. Planificado y perseguido
	3. Bien definido
	4. Controlado cuantitativamente
	5. Continuamente mejorado

Fuente: (The International Systems Security Engineering Association (ISSEA), 2019)

12.4.5.5. Modelo de Evaluación de la Capacidad de Seguridad de CERT/CSO

El modelo CERT/CSO, se encuentra "*centrado en la medición de la calidad relativa a niveles de documentación"* (CSO Online y otros, 2003). Presenta los siguientes cinco niveles de madurez progresiva:

ESQUEMA N°89: Modelo de Madurez del CERT/CSO



Fuente: (CXO Media Inc., 2019)

12.4.5.6. Modelo de madurez de la gestión de la seguridad informática (MMAGSI)

Este curioso Modelo de Madurez de la Gestión de la Seguridad Informática se encuentra basado en “La quinta disciplina” de (Senge P. , 1992), fue desarrollado por Villegas en 2008.

Este modelo establece un contexto con las cinco disciplinas (Senge, Ross, Smith, Roberts, & Kleiner, 2004)*“de las organizaciones inteligentes el dominio personal, los modelos mentales, la visión compartida, el aprendizaje en equipo y el pensamiento sistémico.* “En el siguiente esquema se puede analizar los cinco niveles representados:

ESQUEMA N°90: Modelo de madurez de gestión de la seguridad de la información

Modelo de madurez (basado en Senge P., 1992)				
Inteligencia	Madurez	Desarrollo	Crecimiento	Inicio

Fuente: (Villegas, Modelo de Madurez para la Gestión y Administración de la Seguridad Informática en las Universidades, 2008)

Según (Villegas, Orlando, & Walter, 2009) esta metodología se basa en que:

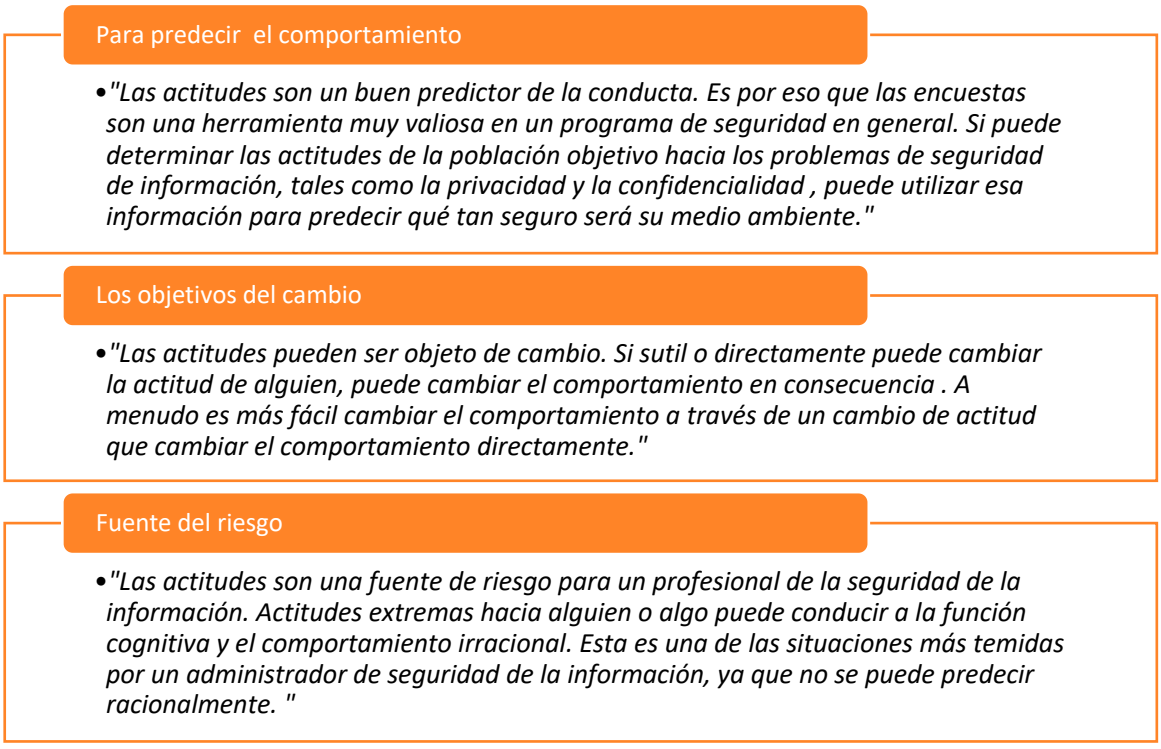
> *"las organizaciones que aprenden tienen institucionalizados procesos de reflexión y aprendizaje en la planificación y evaluación de sus acciones, adquiriendo una nueva competencia (aprender a cómo aprender); lo que implica transformar los modelos mentales vigentes, así como generar visiones compartidas. En tal sentido, bajo esta perspectiva, el MMAGSI es un marco conceptual, que ayuda a los gerentes y trabajadores a comprender la situación de la inseguridad de la información en las organizaciones…"*. (Villegas, Orlando, & Walter, Modelo de Madurez de la Gestión de la Seguridad Informática en el Contexto de las Organizacion es Inteligentes, 2009)

Luego de analizar los modelos de análisis de la cultura en seguridad de la información en entidades bancarias se analizarán las características a considerar en los planes de concientización.

12.4.6. Planes de concientización: características a ser consideradas.

Los autores Tipton H. y Krause M. en su libro: (Information Security Management Handbook, 2005)[xvii] fundamentan que *"las actitudes se definen como nuestra respuesta positiva o negativa a algo."* Asimismo, afirman que los profesionales en seguridad tienen que ser conscientes de las actitudes de los usuarios finales por las siguientes tres razones:

ESQUEMA N°91: Conductas de las personas en un programa de concientización



Fuente: Basado en (Tipton & Krause, Information Security Management Handbook, 2005)

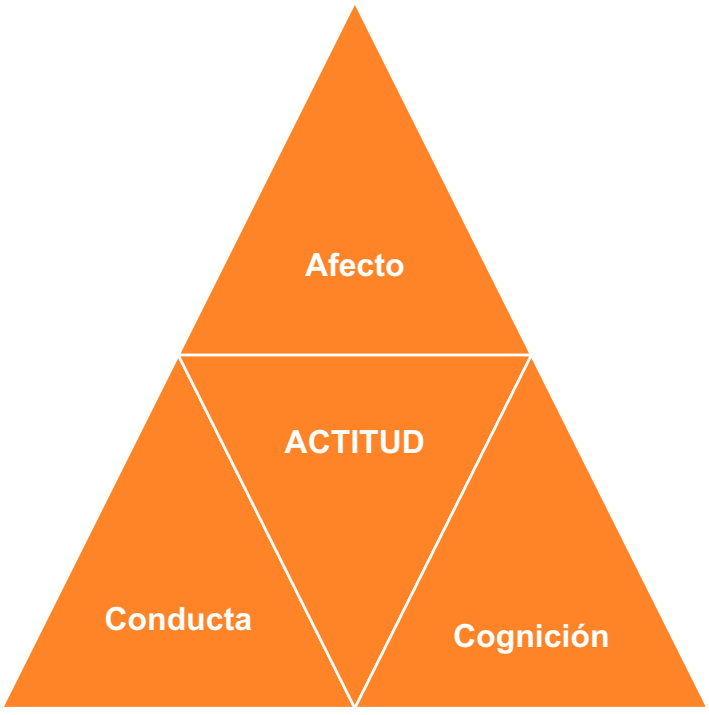
Estas cuestiones hay que tenerlas en cuenta al desarrollar un programa de concientización, porque permiten diagnosticar las conductas de los usuarios y la de

los atacantes en una organización y sienta las bases teóricas para el modelo tripartito en la concientización de la seguridad.

12.4.6.1. El modelo Tripartito del individuo en la Concientización de la Seguridad (Tipton & Krause, Attitude Structure and Function: The ABC's of the Tripartite Model, 2005)[xviii]

Al identificar a los destinatarios del programa de capacitación, existe el modelo tripartito, (también conocido como el modelo ABC), que presenta la actitud como una amalgama de tres componentes medibles separadas: afecto, la conducta y la cognición.

ESQUEMA N°92: El Modelo Tripartito de Concientización de la Seguridad



Fuente: Basado en (Tipton & Krause, Attitude Structure and Function: The ABC's of the Tripartite Model, 2005)

En la siguiente tabla se analizan brevemente cada una de las partes pertinentes del modelo:

ESQUEMA N°93: Modelo Tripartito para analizar al individuo

Modelo		
1	Afecto	*"El componente afectivo es el aspecto emocional de nuestras actitudes. Nuestros sentimientos hacia un objeto o sujeto juegan un papel importante en la determinación de nuestras actitudes."*[xix]
2	Comportamiento	*"El componente de comportamiento se deriva del hecho de que nuestro comportamiento sirve como un mecanismo de retroalimentación para nuestras actitudes. En definitiva, "hacer" conduce a "me gusta"*[xx]*.*
3	Cognición	*"El componente cognitivo es la reflexiva, pensando aspecto de nuestras actitudes".*[xxi]

Fuente: (Tipton & Krause, Attitude Structure and Function: The ABC's of the Tripartite Model, 2005)

Teniendo en cuenta el "afecto" que tienen las personas, el "programa de concienciación sobre la seguridad" puede desarrollarse teniendo en cuenta las respuestas emocionales. Se pueden dar ejemplos, videos o casos de phishing, robo de claves en cajeros automáticos o robo de identidad.

Analizando el comportamiento, se podría enseñar y ejemplificar con el uso de experimentos. Como por ejemplo, cómo se guardan las contraseñas en un Sistema Operativo, cómo los delincuentes utilizan técnicas de skimming para robar datos de

tarjetas de créditos, o reunirlos en grupo para que analicen perfiles en las redes sociales o cómo se incumple con la ley de protección de datos personales en la Argentina.

Y por último, contemplando la Cognición, se los podría hacer reflexionar sobre el manejo y cuidado de la información, en el caso de existir un robo de equipos ya sean notebooks, tabletas o celulares, o ejemplos acerca de cómo se pueden filtrar diferentes videos en la web y causar perjuicios.

12.5. Conclusiones particulares del capítulo XII

Como se analizó en los capítulos anteriores, las normas establecidas por el BCRA, la IGJ, la AAIP, entre otras, impactan en la planificación, gestión y control de los activos de información. Para ello es recomendable la implementación de buenas prácticas y estándares para contribuir a una eficiente administración de los sistemas en las organizaciones; entre los que se destacan:

ESQUEMA N°94: El SAIC y los estándares de análisis de Seguridad de la Información

Estándares y buenas prácticas	Activos de información en custodia de la entidad					
	N1 – Procesos	N2 – Documentación en papel	N3 – Repositorios de archivos y bases de datos	N4 – Plataforma de Software	N5 – Plataforma de Hardware	N6 – Sitios físicos

IRAM/ISO 9001	X	X				
COBIT 5	X			X	X	
Informe COSO	X	X				
IRAM/ISO/IEC 27001	X	X	X	X	X	X
PCI-DSS		X		X		
ITIL	X			X		

Fuente: Elaboración propia.

En el siguiente cuadro comparativo se analizan los modelos de gestión mencionados precedentemente.

ESQUEMA N°95: Análisis de los Modelos de Gestión de la Seguridad de la información y capacitación de los usuarios.

Modelos de Gestión de la Seguridad de la información			
Nombre	**Difusión**	**¿Adapta a las entidades bancarias?**	**Características**
Modelo de Negocio de Seguridad Informática o "The Business Model for Information Security"	Alta	SI	Toma como ejes fundamentales en la gestión de la seguridad a las personas, procesos, tecnologías y organización del ente.

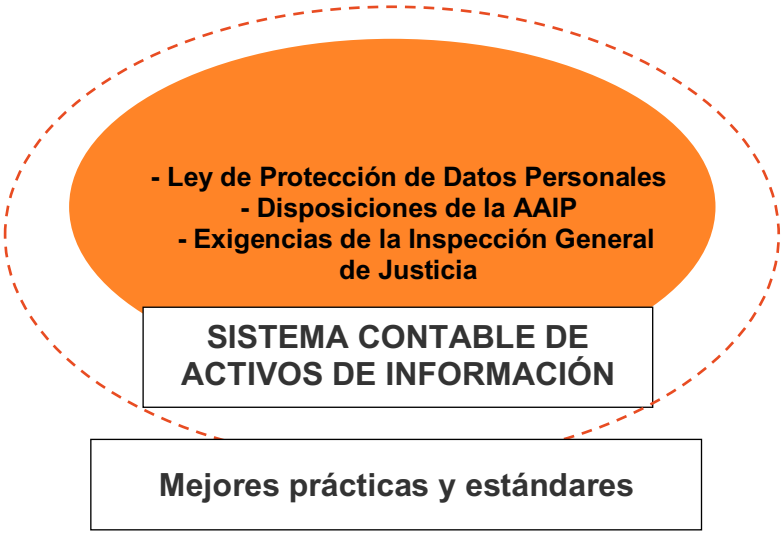
Modelo IRAM/ISO/IEC 27.001	Alta	SI	Establece los lineamientos para implementar un Sistema de Gestión de la Seguridad de la Información.
COBIT	Alta	SI	Está dirigida a la gestión de tecnología de la información (TI).
Modelo Information Security Management Maturity Model (ISM3)	Baja	SI	Se orienta exclusivamente a los sistemas de gestión de calidad IRAM/ISO 9.001.
Modelo Information Security Forum's Standard of Good Practice (SOGP).	Baja	NO	Se basa en buenas prácticas y en las experiencias del ISF (El Foro de Seguridad de la Información).
Modelo ITIL	Media	SI	Se basa en la gestión de los procesos de TI.
Modelo Prince2	Baja	SI	Se orienta a la seguridad relacionada con la gestión de proyectos.
Modelo TLLJO	Baja	NO	Se basa en la implementación de un SGSI, pero permitiendo un mayor control sobre el sistema de costos.
Norma SP800-53 del NIST	Media	SI	Fue tomada como base para la confección de la citada Comunicación “A” 5374/6017 del BCRA.

Fuente: Elaboración propia.

Para el cumplimiento de todas las normas analizadas se establece la necesidad de adoptar procedimientos para administrar eficientemente la Seguridad de la Información en las organizaciones.

A continuación, se puede observar el conjunto de normas relacionadas que impactan en el funcionamiento del sistema contable de activos de información, requiriendo un abordaje interdisciplinario de la seguridad desde un análisis crítico de las herramientas de seguridad implementadas hasta una revisión de las necesidades del negocio en cada entidad bancaria.

ESQUEMA N°96: El sistema de activos de información contable y los estándares de análisis de Seguridad de la Información



Fuente: Elaboración propia.

De las mencionadas, la ISO/IEC/IRAM 27.001 establece un Marco Normativo con los requisitos fundamentales para implementar un sistema de Gestión de Seguridad de la Información, definiendo el objetivo del SGSI como el de "*establecer, implementar, operar, supervisar, revisar, mantener y mejorar*" un sistema de seguridad de la información.

Para la implementación de este resulta necesaria la gestión, implantación de los procesos, procedimientos, documentación, conocimiento de los objetivos y

requisitos para el procesamiento de la información que una organización ha desarrollado para el apoyo a sus operaciones y actividades económicas.

En el caso de los activos de información en custodia de terceras partes, es uno de los puntos más críticos a ser analizados por las entidades bancarias. En esta línea, el BCRA en la Comunicación “A” 6354, estableció dos grandes criterios para analizar la criticidad de los mismos. El primero se relaciona con el tipo de servicio brindado y otro por el tipo de dato suministrado al proveedor:

- **Tipo de servicio:**
  - Infraestructura de Tecnología y Sistemas (SIS)
  - Procesamiento de Datos (SPD)
  - Soporte, Prevención y Mantenimiento (SPM)
  - Comunicaciones (STC)
  - Almacenamiento y Custodia (SAC)
  - Desarrollo de Aplicaciones (SDA)
  - Contingencia y Recuperación (SCR)
- **Tipo de dato**
  - Datos del cliente
  - Datos contables-financieros
  - Datos transaccionales financieros
  - Datos operativos

Desde esta clasificación las entidades deben establecer metodologías para analizar la criticidad de cada uno de sus proveedores.

Finalmente, para poder proteger a los activos de información en conocimiento de los empleados, proveedores y clientes de las entidades bancarias se plantea la necesidad de definir la gestión de la capacitación y concientización en Seguridad Informática.

En el desarrollo del plan de concientización y capacitación, se debe establecer el nivel de madurez que cuenta la entidad y utilizar un modelo de gestión de la capacidad adecuado a la misma. Basándose en la necesidad de resguardar los datos sensibles, las entidades deben analizar los riesgos si los usuarios no reciben la capacitación adecuada para un óptimo cuidado de la información.

A continuación, se analizan los modelos de madurez y los modelos difundidos para gestionar la capacitación y concientización en seguridad:

ESQUEMA N°97: Modelos de madurez cultural de la Seguridad de la Información

Modelos de madurez cultural de la Seguridad de la Información			
Nombre	**Difusión**	**¿Se adapta a las entidades bancarias?**	**Características**
Modelo de Evaluación de la Seguridad de la Información de Citigroup (CITII-SEM)	Alta	SI	Se centra en la concienciación y adaptación por parte de la organización en seguridad.
Modelo de madurez de COBIT	Alta	SI	Se centra en los procedimientos

			específicos de auditoría de COBIT
Modelo de Madurez de Seguridad en TI del NIST-CSEAT	Baja	SI	Se orienta a los niveles de documentación en la organización.
Modelo SSE-CMM	Media	SI	Se basa en la madurez en la ingeniería de seguridad y diseño de software.
Modelo de CERT/CSO	Baja	NO	Se centra en la medición de la calidad relativa a niveles de documentación.
Modelo de Madurez de la Gestión de la Seguridad Informática (MMAGSI)	Baja	SI	Se basa en “La quinta disciplina” de Senge P. (1992).

Fuente: Elaboración propia.

Luego de haber analizado los modelos de evaluación de la madurez y de gestión de la capacitación en la seguridad de la información, se puede destacar que el Modelo CITII-SEM es el único que se centra en concientización en la seguridad, y el modelo de COBIT se centra en los procedimientos específicos de auditoría, lo que permitiría complementarlo con otras normas y actividades de control, por lo tanto, el CITII-SEM es el que más se orienta en la implementación de programas de concientización.

En el análisis de la cultura organizacional se deben tener en cuenta a los usuarios internos y externos para el armado de los contenidos y los programas en concientización de la Seguridad de la Información. Asimismo, resulta necesario que

los mismos se encuentren alineados a las estrategias del negocio, así como contar con la colaboración y apoyo de la alta dirección.

A continuación, se analizarán con las leyes propuestas para los Modelos en la Teoría General Contable y su contrastación con el modelo contable alternativo para los activos de información:

ESQUEMA N°98: Contrastación sobre los Modelos en la Teoría General Contable

Leyes sobre Modelos en la Teoría General Contable enunciados por los autores CLGC, LFG y MCRDM.	Contrastación de las leyes en el contexto de la contabilización de activos de información.
1. La generalización y la abstracción teórica se exterioriza a través de distintos tipos de modelos contables que pretenden representar distintas realidades sociales en las organizaciones.	En la contabilización de los activos de información se puede identificar un modelo contable alternativo que representa lo pertinente a las entidades financieras.
2. Los modelos se estructuran a través de la definición de elementos objetivos y de realidades sociales que pretenden	En el modelo contable alternativo para la contabilización de los activos de información se toman en cuenta los objetivos estratégicos, tácticos y

exteriorizar distintas situaciones en función de los objetivos planteados por distintos usuarios de la información contable.	operativos organizacionales y los establecidos en la disciplina definida como seguridad informática o ciberseguridad.
3. No existe un único modelo capaz de exteriorizar la compleja realidad social de las organizaciones.	En la contabilización de los activos de información se identifica un modelo contable alternativo, pero no significa que sea el más eficiente en describir la realidad en las organizaciones.
4. Los modelos contables exclusivamente patrimoniales se basan en la cuantificación monetaria.	El modelo contable alternativo para la contabilización de los activos de información en entidades financieras no se basa en la cuantificación monetaria.
5. Los modelos contables se pueden definir a partir de elementos que no necesariamente son susceptibles de cuantificación monetaria.	Los elementos descriptos en el modelo contable alternativo para la contabilización de los activos de información en entidades financieras no se basan en la cuantificación monetaria.

Capítulo XIII

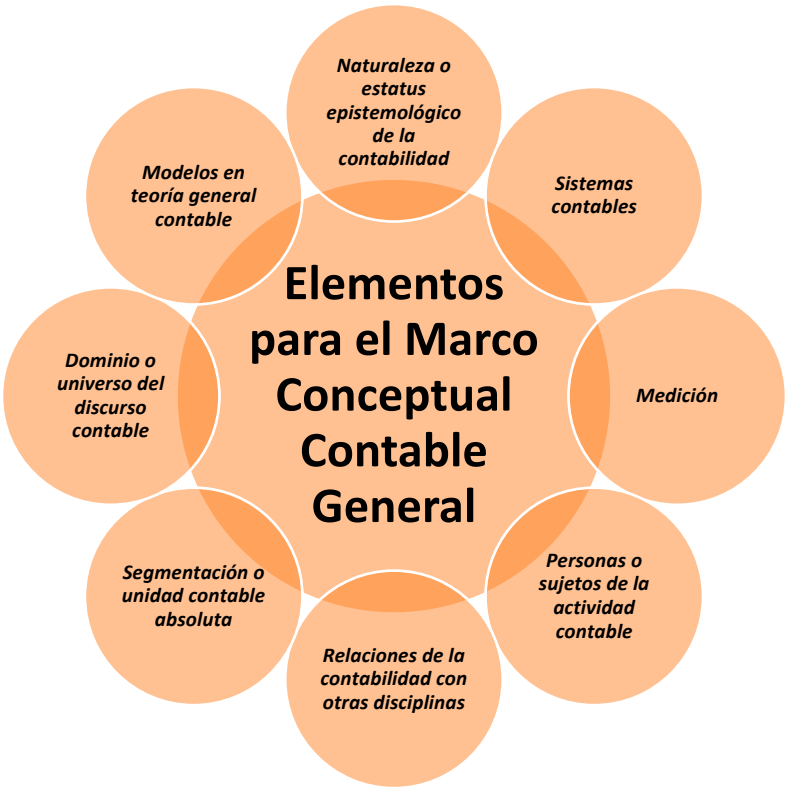
13. Conclusiones

13.1. Introducción

Tomando como base la citada definición de contabilidad propuesta por el Dr. Carlos Luís García Casella, quien la define como: "*una ciencia aplicada factual cultural que se ocupa de la descripción cuantitativa y* [...] *en vista al cumplimiento de sus metas a través de un método basado en un conjunto de supuestos básicos* [...]" (1995), e identificando que se pueden destacar cinco segmentos contables: Contabilidad Financiera, de Gestión, Gubernamental, Nacional y Social-Ambiental; los cuales pueden ser clasificados *"como monetarios y no monetarios y que cada uno de ello se puede desarrollar eficazmente sin ignorar los principios comunes de la Teoría General Contable*" (Barbei , 2017).

Desde esa perspectiva, en la presente tesis se describen los elementos básicos de un Modelo Contable Alternativo para el tratamiento de los activos de información existentes en las entidades bancarias; con características propias del segmento no monetario y cumpliendo las Leyes propuestas para la TGC por los autores (García Casella, Fronti de García, & Rodríguez de Ramírez).

ESQUEMA N°99: Elementos del Marco Conceptual Contable General



Fuente: (García Casella, Fronti de García, & Rodríguez de Ramírez, 2001)

En los siguientes ítems, se expondrán las conclusiones y el análisis de las hipótesis indicadas en la introducción.

13.2. Activos de información

Primera hipótesis propuesta en la presente tesis:

H1: La contabilización de los activos de información existentes en las entidades bancarias conforma un sistema contable con características propias del segmento no monetario.

Contrastación de la hipótesis enunciada:

Se basó en el análisis de las múltiples líneas de investigación abocadas a los diferentes segmentos contables. Puede destacarse que ya desde fines de la década de los sesenta Richard Mattessich identificó a la Contabilidad en dos líneas bien definidas, las que se dedican a la contabilidad monetaria y las que se refieren a la contabilidad no monetaria (Accounting and analytical methods. Measurement and projection of income and wealth in the micro- and macro-economy., 1964). En este contexto y en esta presente investigación se desarrolla el abordaje de los activos de información desde la perspectiva contable no monetaria.

Si bien la definición actual de activo contable establecido en el Marco conceptual de la International Accounting Standards Board (IASB), que lo identifica como:

> "*un recurso económico presente controlado por la entidad como resultado de sucesos pasados.*
>
> *Un recurso económico es un derecho que tiene el potencial de producir beneficios económicos.*
>
> *Aspectos de esas definiciones que se tratan a continuación:*

(a) derechos

(b) potencial de producir beneficios económicos; y

(c) control" (International Accounting Standards Board, El Marco Conceptual para la Información Financiera, 2020).

La información existente en las entidades cumple con los requisitos para ser considerada como tal, pero desde la perspectiva de un modelo contable no monetario, esta definición no contempla el universo de los tipos de información existentes en las entidades.

Considerando la definción de Patrimonio dispuesta por el Dr. Osvaldo Chaves en el desarrollo de la Teoría General Contable, la define *"como el conjunto de bienes, derechos y obligaciones pertenecientes al ente. Cabe agregar que al hablar de bienes y derechos (en principio, activo, en el lenguaje contable) y de obligaciones (pasivo)."* (Chaves, Chyrikins, Dealecsandris, Pahlen Acuña, & Viegas, 1998)

Asimismo, el Dr. Chaves manifiesta que *"para proceder a su distinción se debe considerar en los bienes su mayor o menor grado de convertibilidad en dinero",* y relación a su movilidad, algunos *"le permiten al ente el desarrollo de su actividad específica o le brindan al ente una estructura permanente para facilitar las mencionadas actividades."*

Siguiendo con esta interpretación, en el caso particular de la información no toda posee un valor de cambio cuantificable monetariamente, dado que por las características físicas de la misma se relaciona con el soporte en donde la misma es almacenada. Desde este concepto, se puede definir como una *"*estructura*"* permanente para facilitar las tareas de los entes.

Tomando como base las definiciones precedentes, la información y los datos procesados en las entidades bancarias, se encuentran bajo su custodia y consecuentemente forman parte de los recursos disponibles que poseen. Desde esta interpretación y desde esa contextualización de la TGC, se puede clasificar a la información como un recurso existente en las organizaciones, con un grado de permanencia en el patrimonio.

Desde la posición del autor de la presente tesis, la información cumple con las características del mismo, formando parte del patrimonio de las entidades, dependiendo inevitablemente del soporte de la misma. Los datos en custodia de las entidades constituyen un activo que debería ser identificado, inventariado, administrado y controlado en todas sus formas, ya sea, en datos e información existentes en soporte de papel, en conocimiento de los empleados, o bien resguardados o delegados en terceras partes.

Al interpretar la Teoría del propietario, al caso particular de la contabilización de activos de información, se identifica que existe un interés en las entidades que posee la custodia de la información por sobre la titularidad de otras personas físicas y jurídicas. En este planteo, los particulares de los datos serían ajenos a la información ya que los datos solamente corresponderían a la entidad que tiene su custodia.

Asimismo, al analizar la interpretación de la Teoría de la Entidad al caso particular de la contabilización de activos de información, se identifica la existencia de un conjunto de datos que cuya propiedad no es exclusiva de la entidad, sino, que corresponden a otras personas humanas y jurídicas, y en el caso de las entidades

financieras, estas ejercen el control real de la información. Por lo tanto, la información existente en las entidades corresponde a dos tipos de titulares, los que son titulares y los que poseen la custodia de los datos. En el contexto de la contabilización de los activos de información se identifica que el objetivo de esta Teoría es el proporcionar datos o información útil a quienes controlan los activos de información, sin dejar de brindarle garantías a los titulares de los mismos.

En el marco de la presente tesis, se considera activo de información a todo elemento que contenga, almacene, procese o transmita información de la entidad bancaria. Los mismos pueden ser clasificados según sobre quién recae la custodia de los datos: Activos de información en custodia de la entidad y activos de información en custodia de terceras partes.

Al identificar la información es custodia de las entidades, se pueden destacar:

- **N1 – Procesos:** Corresponde a los macroprocesos, procesos y procedimientos que existen en las entidades.

- **N2 – Documentación en papel:** Corresponde a toda la información existente en formato impreso.

- **N3 – Repositorios de archivos y bases de datos:** Corresponde a todos los archivos de información, repositorios y bases de datos instaladas.

- **N4 – Plataforma de Software:** Corresponde a todos las aplicaciones y sistemas operativos instalados en la entidad.

- **N5 – Plataforma de Hardware:** Comprende a toda la infraestructura de Hardware y Telecomunicaciones existente [xxii] . Ejemplos: Servidores, computadoras de escritorio, computadoras portátiles, teléfonos inteligentes, discos de almacenamiento, etc.

- **N6 – Sitios físicos:** Corresponde a todos los sitios en donde se desarrollan las actividades de la entidad.

Al identificar la información es custodia de terceras partes, se pueden destacar:

- **N7 – Proveedores en servicios centralizados o tercerizados:** En este caso, se identifican todos aquellos servicios de proveedores dedicados al procesamiento, traslado o almacenamiento de datos.

- **N8 – Información en conocimiento del personal:** Corresponde a la información que se encuentra en conocimiento de los Recursos Humanos de la entidad.

En el siguiente esquema se puede identificar el universo de activos de información analizados en la presente investigación.

ESQUEMA N°100: Clasificación de los activos de información según su custodia

Fuente: Elaboración propia.

Si bien con este tipo de definición y clasificación de activos se estaría identificando a toda la información existente en una entidad, se destaca la existencia de interrelaciones e interdependencias entre unos y otros. Cada activo de información posee características propias con vulnerabilidades y amenazas particulares, por lo tanto, corresponde que sean analizadas en forma individual para efectuar un relevamiento completo de los activos de información en las entidades bancarias. En los relevamientos realizados, se identifica la existencia de un sistema de registración de la información en donde la misma es clasificada, analizada y monitoreada siguiendo reglas legales y/o establecidas por organismos de control.

13.3. Naturaleza o estatus epistemológico de la contabilidad, relaciones con otras disciplinas

Segunda hipótesis propuesta en la presente tesis:

H2: La contabilización de los activos de información se relaciona con otras disciplinas como la Tecnología y la Seguridad de la información, sin dependencia de ellas.

Contrastación de la hipótesis enunciada:

La Contabilidad analizada como disciplina es influida por numerosas ciencias básicas y aplicadas, que le aportan nuevas herramientas y características a cumplir para garantizar los requerimientos de la información a los diferentes grupos de interés.

Teniendo en cuenta los requisitos básicos de la seguridad de la información: integridad, confidencialidad y disponibilidad, se puede trazar una estrecha vinculación con lo establecido en el Marco Conceptual de la Información Contable de la RT N°16 de la FACPCE, ya que aporta considerablemente una mejora en los atributos de la información destinada a los usuarios de los Estados Contables o Financieros.

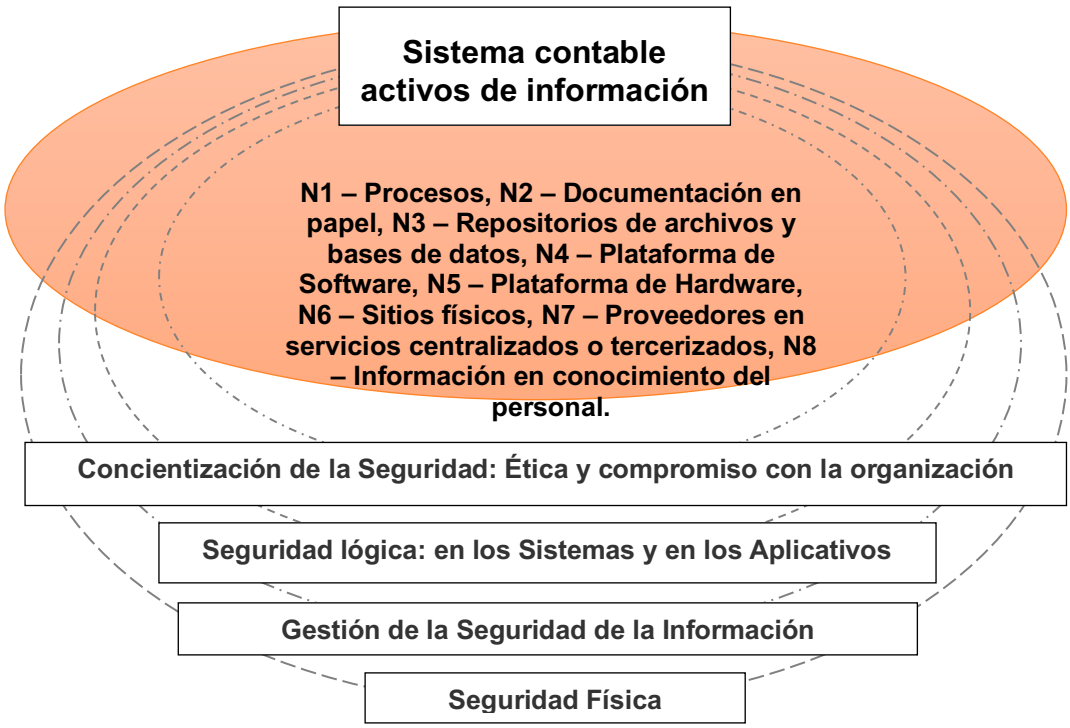
En este análisis, la “Seguridad de la Información” es considerada como una disciplina influyente sobre la contabilidad al contribuir con el cumplimiento de los requisitos de la información contable; dado que brinda los mecanismos específicos y generales para garantizar el cumplimiento de los principios básicos de la

seguridad, impactando en cada uno de los elementos que componen el sistema contable de activos de las entidades bancarias.

Al identificar los elementos básicos que componen un SAIC (Sistema contable de activos de información) se destacan Procesos, Documentación en papel, Repositorios de archivos y bases de datos, Plataforma de Software, Plataforma de Hardware, Sitios físicos, Proveedores en servicios centralizados o tercerizados, Información en conocimiento del personal. En este punto la gestión de la seguridad influye en cada uno de los elementos identificados, desde la seguridad lógica de los aplicativos y sistemas operativos, la seguridad física y hasta la concientización del personal.

En el siguiente esquema se plantean los elementos y los contenidos relacionados con la seguridad de la información:

ESQUEMA N°101: Elementos del SAIC y la Seguridad de la Información



13.4. Sistemas contables de activos de información

Tercera hipótesis propuesta en la presente tesis:

H3: En las entidades bancarias se puede identificar un sistema de información dedicado la recolección y registro de eventos de seguridad y control para los activos de información.

Contrastación de la hipótesis enunciada:

En el contexto de las entidades bancarias se identificó un “sistema contable de activos de información” (SAIC) que brinda información relevante a los siguientes sistemas de gestión: seguridad de la información, calidad, gestión de riesgos y continuidad del negocio, entre otros.

Si bien, el BCRA dispuso en la Comunicación “A” 4609 que las entidades deben tener un registro de los activos de información, el mismo tiene un alcance superior al establecimiento del inventario de activos, dado que para satisfacer las necesidades de los usuarios internos el mismo debería contener mínimamente:

- Registros operativos de las actividades de los usuarios
- Registros de las tareas realizadas
- Registros de las funciones utilizadas
- Reportes de seguridad que registren la asignación de claves y derechos de accesos, empleo de programas de utilidad que permitan el manejo de datos por fuera de las aplicaciones

- Reportes de seguridad de actividades de los usuarios privilegiados
- Reportes de seguridad de usuarios de emergencia y con accesos especiales
- Reportes de seguridad de intentos fallidos de acceso
- Reportes de seguridad de bloqueos de cuentas de usuario
- Reportes de auditoría que registren las excepciones y actividades críticas de las distintas plataformas

Bajo estos requisitos, el sistema de activos de información contable (SAIC) en las entidades bancarias está compuesto mínimamente por los siguientes elementos:

- Tablero de comando / indicadores de Seguridad de la Información.
- Sistema de gestión de información y eventos de seguridad (SIEM)
- Sistema de administración de gestión de bases de datos (CMDB)
- Sistemas de prevención de fuga de información (DLP)
- Inventario de activos de información
- Clasificación de los activos de información
- Información sobre los incidentes de seguridad de la información
- Reportes de la gestión de activos de información

En el siguiente esquema se puede identificar las relaciones del SAIC con los sistemas de gestión.

ESQUEMA N°102: Sistema contable de activos de información (SAIC)

Fuente: Elaboración propia.

13.5. Medición de los activos de información

Cuarta hipótesis propuesta en la presente tesis:

H4: La contabilización de activos de información se ocupa de mediciones cualitativas y cuantitativas no monetarias para poder emitir informes para la toma de decisiones.

Contrastación de la hipótesis enunciada:

Para la identificación de un Modelo Contable particular resulta indispensable establecer criterios de medición acordes al ámbito de aplicación. Dado que el modelo descripto se encuadra dentro de los modelos no monetarios, la medición de estos se realiza con valuaciones cualitativas y con ponderaciones cuantitativas para su análisis.

Una de las metodologías más utilizadas para clasificar la información surge de la serie IRAM/ISO/IEC 27.000 en donde se analiza la criticidad teniendo en cuenta la disponibilidad, confidencialidad e integridad de los datos, con una ponderación para establecer la criticidad y sensibilidad de la información.

Otra de las formas es la establecida por la ley de Habeas Data y las Disposiciones de la Agencia de Acceso a la Información Pública.

En el análisis de los controles establecidos para la clasificación de los activos de información, la IRAM/ISO/IEC 27.002 establece los siguientes puntos de control:

"Directrices de clasificación: *La información debería clasificarse en relación con su valor, requisitos legales, sensibilidad y criticidad para la Organización (…),*

Etiquetado y manipulado de la información: *Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización (…),*

Manipulación de activos: *Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización."*

La normativa analizada destaca la importancia de seleccionar un método con todas las características mínimas a ser consideradas. La normativa establece que los activos de información deben estar etiquetados y recibir el adecuado tratamiento, en base a los datos analizados.

Asimismo, la ley de Habeas Data y las Disposiciones de la Agencia de Acceso a la Información Pública (AAIP) "*han establecido una clasificación de los mismos, en datos básicos, intermedios y sensibles*". (Suarez Kimura & Escobar, Repercusiones de La Ley De Protección de Datos Personales en el Ejercicio Profesional del Contador Público, 2010).

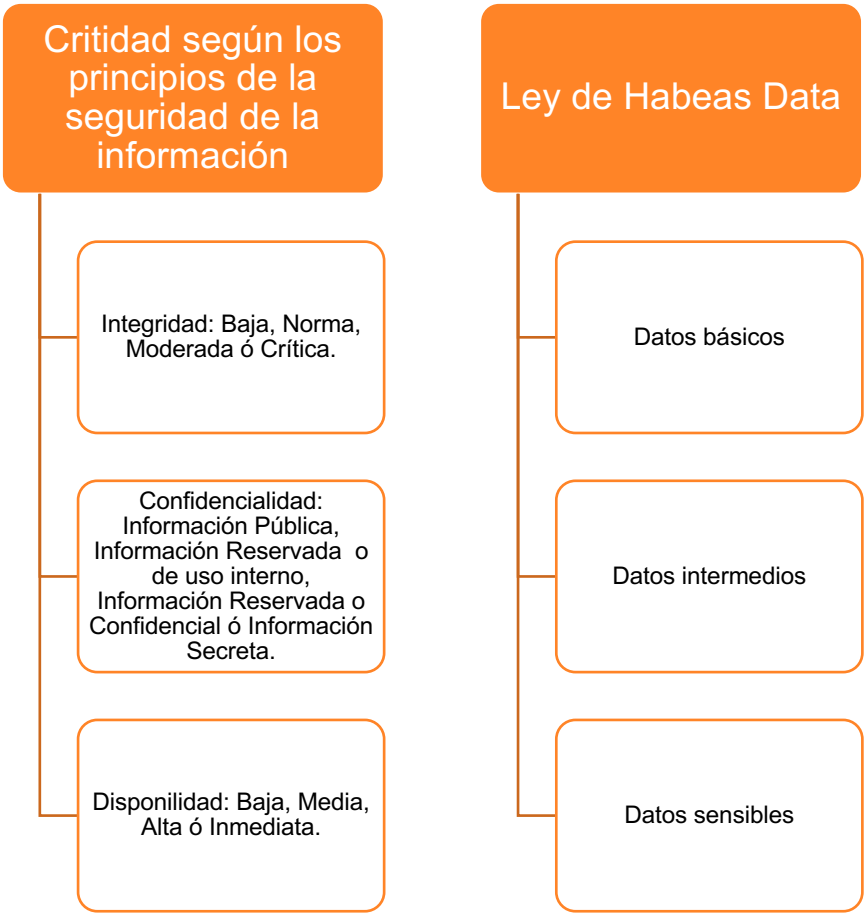
Los datos considerados básicos, corresponden a los existentes en el padrón electoral. Entre ellos encontramos al número de identidad, Nombre y Apellido, CUIT, CUIL, Domicilio, Fecha de Nacimiento, entre otros.

Los datos intermedios son los que superan a los básicos y no son sensibles. Por ejemplo, estado civil, ingresos y egresos, etc.

Los datos sensibles son datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

En el siguiente esquema, se sintetizan las 2 metodologías descriptas para clasificar la información existente en las entidades bancarias.

ESQUEMA N°103: Medición de los activos de información



Fuente: Elaboración propia.

13.6. Personas o sujetos de la actividad contable de activos de información

Quinta hipótesis propuesta en la presente tesis:

H5: En la contabilización de activos de información participan personas o sujetos abocadas a la tarea.

Contrastación de la hipótesis enunciada:

En las entidades bancarias se pueden identificar al conjunto de personas y áreas abocadas a la gestión de activos de información. Las mismas pueden ser agrupadas de la siguiente forma:

- Área responsable de la administración del SAIC
- Áreas relacionadas con la gestión de activos de información
- Áreas de soporte en la gestión de los activos de información
- Áreas y personas usuarias de la información

ESQUEMA N°104: Áreas relacionadas a la contabilización de los activos de información

Fuente: Elaboración propia.

Al analizar la normativa vigente, el BCRA dispuso en la Comunicación “A” 4609 que el área responsable de la gestión de los activos es denominada: “Protección de activos de información”; y la misma “*será responsable de observar la existencia y correcta aplicación de los controles considerados como práctica recomendada y de uso frecuente en la implementación de la protección de los activos*” (BCRA, 2006).

Al analizar en general las incumbencias profesionales en Ciencias Económicas y en particular la del Contador Público, y contextualizado en la presente investigación se puede identificar que en la Ley N°20.488 se establecen como incumbencias del Contador Público: la elaboración e implantación de políticas, sistemas, métodos y procedimientos de trabajo administrativo – contable, como también la aplicación e implantación de sistemas de procesamiento de datos en los aspectos contables y financieros del proceso de información gerencial; relacionando a la profesión en los métodos de procesamientos y soportes que son el contexto de la información contable.

13.7. Dominio o universo del discurso contable

Sexta hipótesis propuesta en la presente tesis:

H6: El universo del discurso contable identificado en el tratamiento de la información en las entidades bancarias, tiene características propias no monetarias, en la identificación, medición, valorización y exposición.

Contrastación de la hipótesis enunciada:

En base a los elementos descriptos por los autores Carlos Luis García Casella, Luisa Fronti de García y María del Carmen Rodríguez de Ramírez en el dominio del discurso contable, en los capítulos de la presente investigación se identificaron:

A- Informes sobre los activos de información de uso interno y externo a los emisores.

B- Personas, grupos de personas y áreas: emisoras de los diversos informes, auditoría que opinan sobre los informes, destinatarias de los diversos informes contables de activos de información.

C- Microsistemas y macrosistemas contables de activos de información propios de cada ente.

D- Modelos contables de activos de información necesarios para determinar variables relevantes en diversas situaciones.

En el universo del discurso contable de los activos de información se identifican regulaciones, estándares y mejores prácticas. A continuación, se detallarán las normativas analizadas y su impacto en la información.

- ✓ **Medidas de control establecidas para resguardar la información financiera en custodia de las entidades bancarias privadas en el Ámbito de la Ciudad Autónoma de Buenos Aires:**

En la actualidad las entidades financieras del ámbito privado poseen sistemas de registros en medios tecnológicos y deben cumplir con los requisitos exigidos por los

organismos de control en cada jurisdicción. Para las que se encuentran radicadas en la CABA, la Inspección General de Justicia describe rigurosas características para dar cumplimiento a la legal forma.

En la Resolución General N°7 del año 2015 se enuncian los requisitos que debe emplearse para la información financiera existente en las entidades bancarias bajo el control de la IGJ. Para obtener la autorización hay que cumplir con los siguientes requisitos relacionados con la seguridad de la información:

- La exposición amplia y precisa del sistema de registración contable a utilizar. Debe incluirse la denominación exacta de los registros que se llevarán mediante el sistema y la de los libros que se reemplazan; y

- Demostración técnica del grado de inalterabilidad de las registraciones a efectuar mediante el sistema propuesto;

Para garantizar la ***inviolabilidad, verosimilitud y completitud*** del sistema de registros se deben analizar los siguientes puntos de control sugeridos:

- Plataforma de Hardware utilizada.

- Plataforma de Software de Base y Aplicaciones utilizadas.

- Políticas de Gestión de Seguridad de la Información.

- Control de Accesos Lógicos y Físicos.

- Back-up / Archivo de la documentación respaldatoria.

- Plan de contingencia.

- Pautas de Confiabilidad.

- Integridad de los Registros Contables.

- ✓ **Habeas data:**

En los sistemas de las entidades bancarias existen numerosas bases de datos en donde se almacena información relacionada con clientes, proveedores y empleados. La Ley N°25.326 establece que las destinadas a proporcionar informes o que procesen información con datos personalizados deben inscribirse en el registro que al efecto habilite el organismo de control.

La información contenida en los sistemas contables no es exclusivamente para uso interno, ya que las entidades utilizan estos datos para realizar diversos reportes como: Estados Financieros, reportes a los organismos de control, informes de responsabilidad social empresaria, de marketing, etc., que son distribuidas a usuarios, sucursales o al holding al cual pertenecen.

La ley plantea que todas las bases de datos están sujetas al reglamento de esta ley, pero la AAIP aconseja registrar las bases de datos que tengan un impacto significativo en la sociedad.

Juntamente con la registración de las bases de datos con información personal, las empresas deben adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, a fin de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

- ✓ **Comunicaciones emitidas por el BCRA:**

Las normas del BCRA que más impactan en la identificación, registración, gestión y control de los activos de información son la “A” 4609 y sus posteriores modificaciones “A” 6017 y la “A” 6354.

En la citada Comunicación “A” 4609, se establecen los requisitos mínimos de gestión, implementación y control de los riesgos relacionados con los sistemas de información, organizando las funciones de las diferentes áreas, estableciendo incompatibilidades y criterios mínimos a establecer.

En la Comunicación “A” 6017 se establecen los requisitos y medidas a implementar en los Canales Electrónicos en donde operan los clientes de las entidades bancarias. Se destaca que la citada norma incluye a la “Concientización y capacitación” de los empleados, clientes y proveedores dentro de los procesos específicos de los mencionados canales.

Y en la Comunicación “A” 6354, se establecen los requisitos mínimos y criterios para analizar la criticidad de los activos de información en custodia de terceras partes. El primero se relaciona con el tipo de servicio brindado y otro por el tipo de dato suministrado al proveedor:

- **Tipo de servicio:**
  - Infraestructura de Tecnología y Sistemas (SIS)
  - Procesamiento de Datos (SPD)
  - Soporte, Prevención y Mantenimiento (SPM)

- Comunicaciones (STC)
- Almacenamiento y Custodia (SAC)
- Desarrollo de Aplicaciones (SDA)
- Contingencia y Recuperación (SCR)

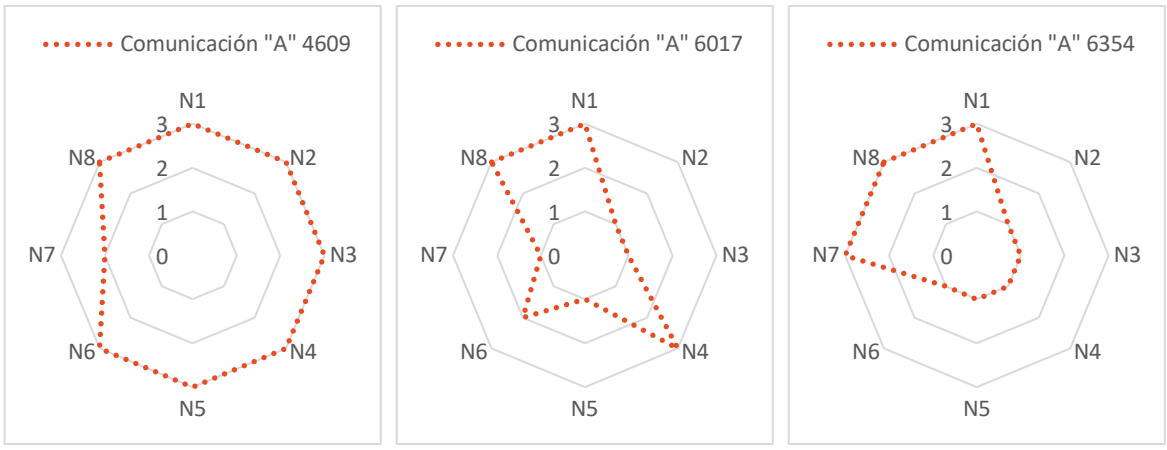
- **Tipo de dato**
  - Datos del cliente
  - Datos contables-financieros
  - Datos transaccionales financieros
  - Datos operativos

Desde esta clasificación las entidades deben establecer metodologías para analizar la criticidad de cada uno de los proveedores.

Con el objetivo de identificar el impacto de cada una de las normas citadas precedentemente en los activos de información, se desarrollaron gráficos radiales en donde se pondera a cada grupo con la siguiente estala: 3- Cuando la normativa tiene un alto impacto en el activo, 2- Cuando la normativa tiene un impacto relativo en el activo, 1- Cuando la normativa no impacta en el activo identificado, 0- Cuando no fue analizado.

En el siguiente esquema se analizan las comunicaciones citadas precedentemente:

ESQUEMA N°105: Comunicaciones del BCRA relacionadas a los activos de información



Fuente: Elaboración propia.

Del análisis realizado, la Comunicación del BCRA que más impacta en los activos es la “A” 4609; le sigue la “A” 6017 referida a los canales electrónicos y por último la “A” 6354, relacionada con los proveedores de servicios de tecnología de información.

- ✓ **Mejores prácticas y estándares de control y gestión**

Como se analizó en los capítulos anteriores, las normas establecidas por el BCRA, la IGJ, la AAIP, entre otras, impactan en la planificación, gestión y control de los activos de información. Para ello es recomendable la implementación de buenas prácticas y estándares para contribuir a una eficiente administración de los sistemas en las organizaciones; entre los que se destacan:

- Estándares de control
- Modelos de gestión de la seguridad de la información

- Modelos de madurez de la gestión de los activos de información

En el siguiente esquema se identifican los estándares aplicables en la gestión de activos de información en custodia de la entidad.

ESQUEMA N°106: El sistema de activos de información contable y los estándares de análisis de Seguridad de la Información

Activos de información en custodia de la entidad	Estándares y buenas prácticas					
	IRAM/ISO 9001	COBIT 5	Informe COSO	IRAM/ISO/IEC 27001	PCI-DSS	ITIL
N1 – Procesos	X	X	X	X		X
N2 – Documentación en papel	X		X	X	X	
N3 – Repositorios de archivos y bases de datos				X		
N4 – Plataforma de Software		X		X	X	X

N5 – Plataforma de Hardware		X		X		
N6 – Sitios físicos				X		

Fuente: Elaboración propia.

Para el cumplimiento de todas las normas analizadas se establece la necesidad de adoptar procedimientos para administrar eficientemente la Seguridad de la Información en las organizaciones.

En el siguiente esquema se detallan los modelos de gestión aplicables a la seguridad y capacitación de los usuarios.

ESQUEMA N°107: Análisis de los Modelos de Gestión de la Seguridad de la información y capacitación de los usuarios.

Modelos de Gestión de la Seguridad de la información		
Nombre	**Difusión**	**¿Adapta a las entidades bancarias?**
Modelo de Negocio de Seguridad Informática o "The Business Model for Information Security"	Alta	SI

Modelo IRAM/ISO/IEC 27.001	Alta	SI
COBIT	Alta	SI
Modelo Information Security Management Maturity Model (ISM3)	Baja	SI
Modelo Information Security Forum's Standard of Good Practice (SOGP).	Baja	NO
Modelo ITIL	Media	SI
Modelo Prince2	Baja	SI
Modelo TLLJO	Baja	NO
Norma SP800-53 del NIST	Media	SI

Fuente: Elaboración propia.

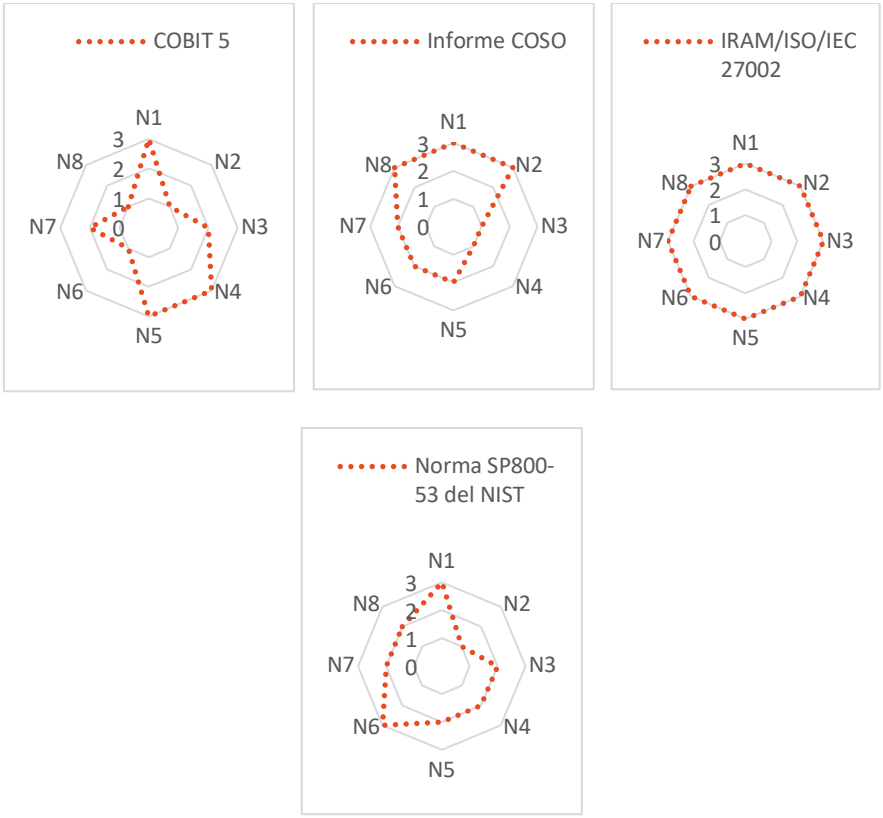
Con el objetivo de identificar las relaciones de la normativa con los activos de información existentes se desarrollaron gráficos radiales, en donde se pondera con la escala: 3- Cuando el modelo identifica al activo, 2- Cuando el modelo identifica indirectamente al activo, 1- Cuando el modelo no alcanza al activo analizado, 0- Cuando no fue analizado.

ESQUEMA N°108: Modelos de Gestión de la Seguridad de la Información

Fuente: Elaboración propia.

De los modelos de gestión analizados, el establecido por la IRAM/ISO/IEC 27.001 es que se adapta y contempla a todos los activos de información propuestos.

ESQUEMA N°109: Estándares relacionados con el control de la Seguridad de la Información



Fuente: Elaboración propia.

En base a los estándares de control identificados la norma IRAM/ISO/IEC 27.002 es la que establece controles relacionados con todos los activos de información.

Para poder proteger a los activos en conocimiento de los empleados, proveedores y clientes de las entidades bancarias se plantea la necesidad de definir la gestión de la capacitación y concientización en Seguridad Informática.

En el desarrollo de este plan se debe establecer el nivel de madurez que cuenta la entidad y utilizar un modelo de gestión de la capacidad adecuado a la entidad. Basándose en la necesidad de resguardar los datos sensibles, las entidades deben analizar los riesgos si los usuarios no reciben la capacitación adecuada para un óptimo cuidado de los datos.

En el siguiente esquema se detallan los modelos de madurez y los modelos difundidos para gestionar la capacitación y concientización en seguridad de la información.

ESQUEMA N°110: Modelos de madurez cultural de la Seguridad de la Información

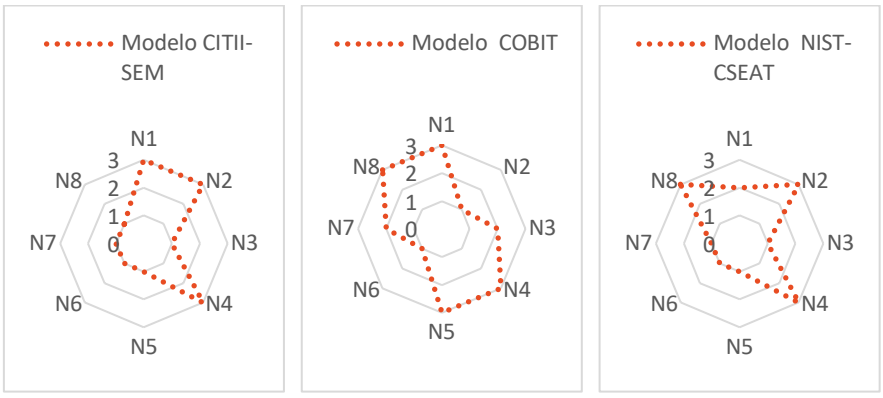
Modelos de madurez cultural de la Seguridad de la Información		
Nombre	**Difusión**	**¿Se adapta a las entidades bancarias?**
Modelo de Evaluación de la Seguridad de la Información de Citigroup (CITII-SEM)	Alta	SI
Modelo de madurez de COBIT	Alta	SI
Modelo de Madurez de Seguridad en TI del NIST-CSEAT	Baja	SI
Modelo SSE-CMM	Media	SI

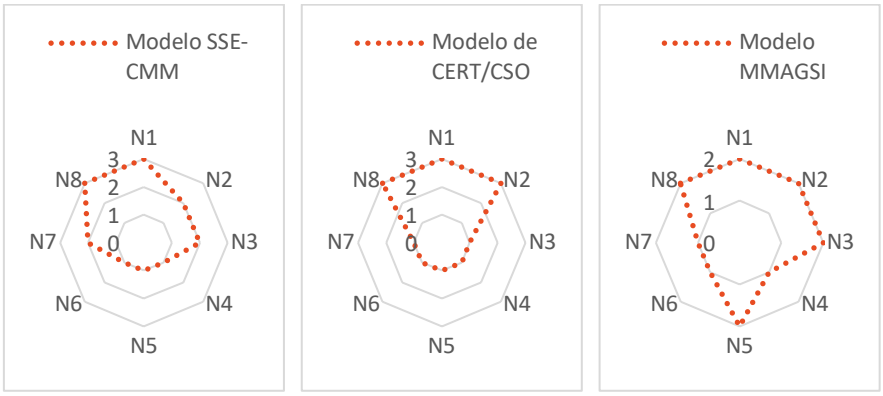
Modelo de CERT/CSO	Baja	NO
Modelo de Madurez de la Gestión de la Seguridad Informática (MMAGSI)	Baja	SI

Fuente: Elaboración propia.

De los modelos analizados, el modelo de madurez de Cobit es el que permite cubrir más eficazmente la gestión y el control de los activos de información. A continuación, se analizan los citados modelos:

ESQUEMA N°111: Modelos de análisis de la madurez de los sistemas de gestión de Seguridad de la Información





Fuente: Elaboración propia.

Luego de haber analizado los modelos de evaluación de la madurez y de gestión de la capacitación en la seguridad de la información, el Modelo CITII-SEM es el único que se centra en concientización en la seguridad y el modelo de COBIT se centra en los procedimientos específicos de auditoría, lo que permitiría complementarlo con otras normas y actividades de control, por lo tanto, el CITII-SEM es el que más se orienta en la implementación de programas de concientización.

En el análisis de la cultura organizacional se deben tener en cuenta a los usuarios internos y externos para el armado de los contenidos y los programas en concientización. Asimismo, resulta necesario que los mismos se encuentren alineados a las estrategias del negocio, así como contar con la colaboración y apoyo de la alta dirección.

13.8. Modelo contable alternativo de activos de información

Séptima hipótesis propuesta en la presente tesis:

H7: La contabilización de activos de información en las entidades bancarias cumple con todos los requisitos para ser considerado un modelo contable alternativo del segmento no monetario.

Contrastación de la hipótesis enunciada:

A través del desarrollo de cada uno de los capítulos precedentes se han considerado los elementos a incluir a la hora de plantear un modelo contable que contemple expresamente a los activos de información de una entidad bancaria. Se destacan los siguientes elementos analizados:

- **Dominio del discurso contable:** En el ámbito de las instituciones bancarias se identificaron: Informes sobre los activos de información de uso interno y externo a los emisores. Sujetos y áreas abocadas a las tareas de las mismas, y estándares o buenas prácticas específicas para cada activo de información.

- **Naturaleza o estatus epistemológico de la contabilidad:** Desde la perspectiva de la contabilización de activos de información, la contabilidad debe ser concebida desde la definición de García Casella como una ciencia factual cultural.

- **Sistemas contables:** En la contabilización de los activos de información en entidades bancarias se observan microsistemas propios de cada ente y macrosistemas que corresponden al Estado.

- **Medición:** En la contabilización de los activos de información se identificaron criterios de medición no monetarios basados en la criticidad de la información o en la clasificación establecida en la Ley de Habeas Data.

- **Personas o sujetos de la actividad contable**: En la contabilización de los activos de información se identificaron personas, grupos de personas y áreas específicas: emisoras de los diversos informes, que realizan procedimientos de auditorías, que opinan sobre los informes y destinatarias de los diversos informes.

- **Relaciones de la contabilidad con otras disciplinas:** En la contabilización de los activos de información se relaciona con otras disciplinas como la Tecnología y la Seguridad de la información.

- **Segmentación contable:** La contabilización de los activos de información en entidades bancarias cumple con las características del segmento contable no monetario.

- **Modelos de la teoría general contable:** Por todo lo expuesto y en base a los elementos de la TGC analizados precedentemente, se arriba a la identificación de los elementos básicos de un Modelo Contable Alternativo no monetario para los activos de información existentes en las entidades financieras.

Anexo

Anexo I

14. Propuesta de metodología de selección de proveedores utilizando metodologías borrosas.

14.1. Introducción

El presente anexo tiene por objetivo principal proponer una metodología de selección de proveedores utilizando metodologías borrosas. A continuación, se presentan los objetivos particulares a tratar:

- Identificar los proveedores de este servicio en el ámbito de la República Argentina.
- Seleccionar diez características de los proveedores para ser evaluados.

- Construir una matriz de incidencia del conjunto de las características en el mismo conjunto y luego analizar si existen efectos olvidados.
- Ordenar los proveedores por grupos de afinidad teniendo en cuenta las características comunes a un nivel dado.
- Valorar las características de cada proveedor y establecer un criterio para seleccionar el más adecuado.

14.2. Elementos de conjuntos borrosos

En la presente sección se analizarán las principales características de las herramientas borrosas utilizadas en trabajo.

14.2.1. Marco Teórico de conjuntos Borrosos

Los conjuntos borrosos o difusos nacieron con este nombre en 1965, a partir del artículo del profesor de Ingeniería Electrónica de la Universidad de California en Berkeley y fundador de la teoría, Lofti A. Zadeh. Él "*amplió la teoría clásica de conjuntos para poder operar con clases definidas por predicados vagos y logró esa ampliación generalizando el concepto de pertenencia a un conjunto A para el que sólo existían, a ese momento, dos posibilidades: x pertenece a A o x no pertenece a A, que expresado mediante la función característica o de elección de Boole respectivamente. Zadeh introdujo la idea de los conjuntos borrosos, caracterizados por funciones características generalizadas o funciones de pertenencia* μ_A*, cuyos valores no son sólo los números 0 y 1, sin o todos los números entre 0 y 1; la*

pertenencia dejó de ser abrupta para ser graduada". (Lazzari, Marachado, & Perez, Matemática Borrosa, Técnicas de Gestión para el tratamiento de la incertidumbre. , 1998)

14.2.2. Conjunto Borroso

Para definir a un conjunto borroso, utilizamos la siguiente definición:

Sea *X* un universo continuo o discreto.

Un **subconjunto borroso** o ***fuzzy set*** $\mu_{\tilde{A}} : X \to [0,1]$

$\mu_{\tilde{A}}(x)$ *grado* o **nivel de pertenencia** de *x* a $\tilde{A}$

α- corte o **conjunto de nivel** α de *A*

$$A_\alpha = \{x \in X / \mu_{\tilde{A}}(x) \geq \alpha\} \qquad \alpha \in (0,1]$$

Fuente: (Mouliá & Lazzari, 2012)

14.2.3. Matriz de efectos olvidados

Los efectos olvidados son "aquellos mecanismos de causa a efecto que no es posible encontrar a través de la intuición o de la experiencia. Generalmente no han sido previstos y considerados cuando se han tomado decisiones, pero se manifiestan más tarde frecuentemente disimulados y a veces de manera drástica."

(Lazzari, Marachado, & Perez, Matemática Borrosa, Técnicas de Gestión para el tratamiento de la incertidumbre. , 1998)

A partir de las matrices de incidencia borrosas se intenta descubrir algunos efectos no tenidos en cuenta cuando se produce la toma de decisiones.

14.2.4. Agrupación por afinidad

La noción de afinidad surge a partir de la necesidad de poder abordar el estudio de relaciones representadas a través de matrices rectangulares que permiten vincular los elementos de un conjunto con los de otro. (Kaufmann & Gil-Aluja, 1991)

> *"Aspectos que configuran este concepto:*
>
> *i) La homogeneidad de cada agrupación debe vincularse al nivel elegido que funciona como umbral a partir del cual se busca la afinidad.*
>
> *ii) Los elementos de uno de los conjuntos deben estar ligados con los del otro por ciertas reglas.*
>
> *iii) Debe existir una estructura constitutiva de un cierto orden que permita la posterior decisión."*

Para el cálculo y análisis de las afinidades, se estableció los siguientes pasos:

Sea $\widetilde{R} : H \times T \to [0,1]$

i) "Establecer un grado mínimo a partir del cual se considera la existencia de afinidad para cada característica que determina un límite o umbral $\alpha \in (0,1]$.

ii) Obtener el α*-corte de la relación* $\widetilde{R}$ *:*

$$R_\alpha = \left\{ (x,y) \in H \times T \,/\, \mu_{\tilde{R}}(x,y) \geq \alpha \right\}, \alpha \in (0,1]$$

R_α *es una relación binaria crisp.*

iii) Elegir entre H y T el conjunto que posee menor número de elementos.

iv) Calcular el conjunto potencia de H (si es el elegido). El cardinal de este conjunto es $\#(\wp(H)) = 2^n$ *, n es el número de elementos de H.*

v) Hacer corresponder a cada elemento de $\wp(H)$ *aquellos elementos de T con los cuales está relacionado a nivel mayor o igual que el seleccionado.*

vi) Descartar los subconjuntos vacíos y los subconjuntos incluidos en otro.

Los subconjuntos resultantes son las llamadas subrelaciones de afinidad, que forman un retículo de Galois.

Los elementos de T (o de H) quedan agrupados por características comunes a nivel mayor o igual que el elegido." (Lazzari, Moulia, & Fogel, AGRUPACIÓN DE PRODUCTOS FINANCIEROS POR AFINIDAD, 2012)

En base a estas herramientas borrosas se analizarán los proveedores en la siguiente sección.

14.3. Análisis de los proveedores

En base a lo analizado precedentemente, en la presente sección observaremos los proveedores existentes en la República Argentina que brindan este tipo de servicio, y luego serán seleccionados mediante herramientas de la metodología borrosa.

14.3.1. Identificación de los proveedores en el ámbito de la República Argentina

En marco del presente trabajo y mediante una búsqueda en el ámbito de la República Argentina, se identificaron los siguientes 16 proveedores:

$$P = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}, p_{15}, p_{16}\}$$

Los mismos serán utilizados en los puntos posteriores. A continuación se establecerán las características para el análisis de cada uno.

14.3.2. Características para evaluar a los proveedores

Características de los proveedores seleccionados se escogieron las siguientes para analizarlos:

ESQUEMA N°112: Características para analizar proveedores

Características para analizar proveedores	
c_1	Cargos Fijos
c_2	Cargos Variables
c_3	Tipo de moneda a facturar
c_4	Idioma del soporte

c_5	Ubicación de las oficinas comerciales
c_6	Ubicación de los datacenters principales
c_7	Reputación en el mercado
c_8	Certificación de normas ISO
c_9	Planes de continuidad operativa
c_{10}	Disponibilidad operativa garantizada

Fuente: Elaboración Propia.

$$C = \{c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9, c_{10}\}$$

14.3.3. ANÁLISIS DE EFECTOS OLVIDADOS EN LAS INCIDENCIAS ENTRE LAS CARACTERÍSTICAS DE LOS PROVEEDORES

En el presente apartado se construirá una matriz de incidencia del conjunto de las características en el mismo conjunto, de acuerdo con la opinión de expertos en el tema.

Posteriormente se analizará la posible existencia de efectos olvidados y se buscarán las incidencias intermedias.

A continuación, se representan las matrices de incidencia utilizando las citadas características.

ESQUEMA N°113: Matriz de incidencia de primer orden

R ~	Cargos Fijos	Cargos Variables	Tipo de moneda a facturar	Idioma del soporte	Ubicación de las oficinas comerciales	Ubicación de los datacenters principales	Reputación en el mercado	Certificación de normas ISO	Planes de continuidad operativa	Disponibilidad operativa garantizada
Cargos Fijos	1	0,5	0,5	0	0	0	0	0	0	0
Cargos Variables	0,5	1	0,5	0	0	0	0	0	0	0
Tipo de moneda a facturar	0,5	0,5	1	0,3	0,7	0,6	0	0	0	0
Idioma del soporte	0	0	0,7	1	0,6	0,5	0	0	0	0
Ubicación de las oficinas comerciales	0	0	0,7	0,8	1	0,8	0,6	0,1	0,2	0,1
Ubicación de los datacenters principales	0,7	0,7	0,9	0,7	0,9	1	0,5	0,4	0,3	0,1
Reputación en el mercado	0,2	0,2	0	0	0	0	1	0,5	0,4	0
Certificación de normas ISO	0	0	0	0	0	0	0,5	1	0,4	0,5
Planes de continuidad operativa	0	0	0	0	0	0,4	0,7	0,8	1	0,9
Disponibilidad operativa garantizada	0	0	0	0	0	0,5	0,3	0,6	0,9	1

Fuente: Elaboración Propia.

ESQUEMA N°114: Matriz de unión de los efectos de primera y segunda generación

R2 ~	Cargos Fijos	Cargos Variables	Tipo de moneda a facturar	Idioma del soporte	Ubicación de las oficinas comerciales	Ubicación de los datacenters principales	Reputación en el mercado	Certificación de normas ISO	Planes de continuidad operativa	Disponibilidad operativa garantizada
Cargos Fijos	1	0,5	0,5	0,3	0,5	0,5	0	0	0	0
Cargos Variables	0,5	1	0,5	0,3	0,5	0,5	0	0	0	0
Tipo de moneda a facturar	0,6	0,6	1	0,7	0,7	0,7	0,6	0,4	0,3	0,1
Idioma del soporte	0,5	0,5	0,7	1	0,7	0,6	0,6	0,4	0,3	0,1
Ubicación de las oficinas comerciales	0,7	0,7	0,8	0,8	1	0,8	0,6	0,5	0,4	0,2
Ubicación de los datacenters principales	0,7	0,7	0,9	0,8	0,9	1	0,6	0,5	0,4	0,4
Reputación en el mercado	0,2	0,2	0,2	0	0	0,4	1	0,5	0,4	0,5
Certificación de normas ISO	0,2	0,2	0	0	0	0,5	0,5	1	0,5	0,5
Planes de continuidad operativa	0,4	0,4	0,4	0,4	0,4	0,5	0,7	0,8	1	0,9
Disponibilidad operativa garantizada	0,5	0,5	0,5	0,5	0,5	0,5	0,7	0,8	0,9	1

Fuente: Elaboración Propia.

ESQUEMA N°115: Matriz de efectos de segunda generación

R2 - R ~ ~	Cargos Fijos	Cargos Variables	Tipo de moneda a facturar	Idioma del soporte	Ubicación de las oficinas comerciales	Ubicación de los datacenters principales	Reputación en el mercado	Certificación de normas ISO	Planes de continuidad operativa	Disponibilidad operativa garantizada
Cargos Fijos	0	0	0	0,3	0,5	0,5	0	0	0	0
Cargos Variables	0	0	0	0,3	0,5	0,5	0	0	0	0
Tipo de moneda a facturar	0,1	0,1	0	0,4	0	0,1	0,6	0,4	0,3	0,1
Idioma del soporte	0,5	0,5	0	0	0,1	0,1	0,6	0,4	0,3	0,1
Ubicación de las oficinas comerciales	0,7	0,7	0,1	0	0	0	0	0,4	0,2	0,1
Ubicación de los datacenters principales	0	0	0	0,1	0	0	0,1	0,1	0,1	0,3
Reputación en el mercado	0	0	0,2	0	0	0,4	0	0	0	0,5
Certificación de normas ISO	0,2	0,2	0	0	0	0,5	0	0	0,1	0
Planes de continuidad operativa	0,4	0,4	0,4	0,4	0,4	0,1	0	0	0	0
Disponibilidad operativa garantizada	0,5	0,5	0,5	0,5	0,5	0	0,4	0,2	0	0

Fuente: Elaboración Propia.

Estableciendo como límite 0,7 para este análisis, se puede observar que existen efectos olvidados en las incidencias de la “ubicación de las oficinas comerciales” en los “cargos fijos” y en los “cargos variables” de los proveedores. A continuación, se analizarán las incidencias intermedias.

- Análisis de la incidencia intermedia de la ubicación de las oficinas comerciales y los cargos fijos:

ESQUEMA N°116: Análisis de la incidencia intermedia

Ubicación de las oficinas comerciales	**0**	**0**	**0,7**	**0,8**	**1**	**0,8**	**0,6**	**0,1**	**0,2**	**0,1**
Cargos Fijos	**1**	**0,5**	**0,5**	**0**	**0**	**0,7**	**0,2**	**0**	**0**	**0**
Min	**0**	**0**	**0,5**	**0**	**0**	**0,7**	**0,2**	**0**	**0**	**0**

Fuente: Elaboración Propia.

Valores máximos: {C_6}

La incidencia intermedia es la C_5, la ubicación de los datacenters, por lo tanto, la ubicación de las oficinas comerciales incide por la ubicación de los datacenters en los cargos fijos.

- Análisis de la incidencia intermedia de la ubicación de las oficinas comerciales y los cargos variables:

ESQUEMA N°117: Análisis de la incidencia intermedia

Ubicación de las oficinas comerciales	0	0	0,7	0,8	1	0,8	0,6	0,1	0,2	0,1
Cargos Variables	0,5	1	0,5	0	0	0,7	0,2	0	0	0
Min	0	0	0,5	0	0	0,7	0,2	0	0	0

Fuente: Elaboración Propia.

Valores máximos: {C6}

La incidencia intermedia es la C_6, la ubicación de los datacenters, por lo tanto, la ubicación de las oficinas comerciales incide por la ubicación de los datacenters en los cargos variables.

Con el objetivo de cuantificar la información suministrada se desarrollaron las siguientes escalas para la cuantificación de cada una de las características planteadas:

ESQUEMA N°118: Escala de Costos Fijos

Costo Fijo	
0 =< 1000	1

1001 > 2000	0,9
2001 > 3000	0,8
3001 > 4000	0,7
4001 > 5000	0,6
5001 > 6000	0,5
6001 > 7000	0,4
7001 > 8000	0,3
8001 > 9000	0,2
9001 > 10000	0,1
10001 <	0

Fuente: Elaboración Propia.

ESQUEMA N°119: Escala de costos variables

Costo Variable	
0 < 2700	1
2701 < 3900	0,9
3901 < 5100	0,8
5101 < 6300	0,7

6301 < 7500	0,6
7501 < 8700	0,5
8701 < 9900	0,4
9901 < 11100	0,3
11101 < 12300	0,2
12301 < 13500	0,1
13501 >	0

Fuente: Elaboración Propia.

ESQUEMA N°120: Escala de tipo de moneda a facturar

Tipo de moneda a facturar	
Pesos Argentinos	1
Dólares Estadounidenses	0,75
Euros	0,5
Otras	0,25

Fuente: Elaboración Propia.

ESQUEMA N°121: Escala de idioma del soporte

Idioma del soporte	
Español	1
Inglés	0,66
Portugués	0,33
Otros	0

Fuente: Elaboración Propia.

ESQUEMA N°122: Escala de ubicación de las oficinas comerciales

Ubicación de las oficinas comerciales	
Argentina	1
Latinoamérica	0,75
Europa	0,5
Norte de américa	0,25
Resto del mundo	0

Fuente: Elaboración Propia.

ESQUEMA N°123: Escala de ubicación de los datacenters

Ubicación de los datacenters principales	
Argentina	1
Países recíprocos con la LPDP	0,5
Otros países no recíprocos con la LPDP	0

Fuente: Elaboración Propia.

ESQUEMA N°124: Escala de reputación en el mercado

Reputación en el mercado	
Más de 10	1
Entre 10 y 5 años	0,5
Entre 5 y 2 años	0,25
Menos de 2 años	0

Fuente: Elaboración Propia.

ESQUEMA N°125: Escala de certificación de normas ISO

Certificación de normas ISO	
ISO 9001 – 20001 – 27001	1
ISO 27001	0,8
ISO 9001 – 20001	0,6
ISO 9001	0,4
ISO 20001	0,2
No tiene normas certificadas	0

Fuente: Elaboración Propia.

ESQUEMA N°126: Escala de Planes de continuidad operativa

Planes de continuidad operativa	
Planes Documentados y formalizados	1
Planes Documentados	0,66
Planes informales	0,33
Sin planes Documentados y formalizados	0

Fuente: Elaboración Propia.

ESQUEMA N°127: Escala de disponibilidad operativa garantizada

Disponibilidad operativa garantizada	
99,99	1
99,9	0,8
99,5	0,6
99,1	0,4
99	0,2
Menos de 99	0

Fuente: Elaboración Propia.

Al cuantificar cada una de las variables analizadas, se obtiene la siguiente tabla de proveedores que será utilizada para su selección.

14.3.4. Agrupación de los proveedores por afinidad:

Para una mejor selección de proveedores, en el presente segmento se analizará el agrupamiento de los mismos, teniendo en cuenta las características que poseen. La noción de afinidad *"surge a partir de la necesidad de poder abordar el estudio de relaciones representadas a través de matrices rectangulares que permiten vincular los elementos de un conjunto con los de otro."* (Kaufmann & Gil-Aluja, 1991)

Considerando opciones de proveedores seleccionados:

$$P = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}, p_{15}, p_{16}\}$$

Y las características presentadas:

$$C = \{c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9, c_{10}\}$$

C1: Cargos Fijos.

C2: Cargos Variables.

C3: Tipo de moneda a facturar.

C4: Idioma del soporte.

C5: Ubicación de las oficinas comerciales.

C6: Ubicación de los datacenters principales.

C7: Reputación en el mercado.

C8: Certificación de normas ISO.

C9: Planes de continuidad operativa.

C10: Disponibilidad operativa garantizada.

14.3.5. Clasificación y selección de proveedores

En base a la matriz de proveedores, y en base a un criterio de expertos se establece el siguiente grado de importancia de cada característica considerada:

ESQUEMA N°128: Ponderación de las características

Ponderación de las características	
Cargos Fijos	**0,1**
Cargos Variables	0,15
Tipo de moneda a facturar	0,05
Idioma del soporte	0,05
Ubicación de las oficinas comerciales	0,15
Ubicación de los datacenters principales	0,2
Reputación en el mercado	0,05
Certificación de normas ISO	0,1
Planes de continuidad operativa	0,1
Disponibilidad operativa garantizada	0,05
Total	1

Utilizando las características cuantificadas en la matriz de proveedores se obtiene la matriz de valuaciones. Para ello, se multiplicó la ponderación, a cada de las características de los proveedores.

14.4. Conclusiones particulares del Anexo I

Luego de haber definido los conceptos de conjuntos borrosos e identificados 16 proveedores (los cuales brindan estos servicios para el resguardo de información contable en base a esa tecnología); se seleccionaron las siguientes diez características para que los mismos sean evaluados:

c1 Cargos Fijos

c2 Cargos Variables

c3 Tipo de moneda a facturar

c4 Idioma del soporte

c5 Ubicación de las oficinas comerciales

c6 Ubicación de los datacenters principales

c7 Reputación en el mercado

c8 Certificación de normas ISO

c9 Planes de continuidad operativa

c10 Disponibilidad operativa garantizada

Para analizar si existen efectos olvidados en la selección de las características, se realizaron las matrices correspondientes para identificar “efectos de segunda generación”, en donde se hallaron 2 efectos: el primero radica en que la ubicación de los datacenters, por la ubicación de las oficinas comerciales incide en los cargos

fijos; y el segundo la ubicación de las oficinas comerciales incide por la ubicación de los datacenters en los cargos variables. Dichos efectos fueron adecuados en el análisis.

En una segunda instancia, se ordenaron los proveedores por grupos de afinidad teniendo en cuenta las características comunes a un nivel dado. El subconjunto de proveedores compuesto por {p11, p12, p13, p14} es el que cumple con la mayor cantidad de características solicitadas a nivel mayor o igual que 0.8: C1: Cargos Fijos; C2: Cargos Variables; C3: Tipo de moneda a facturar; C4: Idioma del soporte; C5: Ubicación de las oficinas comerciales y C6: Ubicación de los datacenters principales. Esta agrupación fue tenida en cuenta en la selección del proveedor óptimo.

Para valorar las características de cada proveedor y establecer un criterio de expertos se establece el siguiente grado de importancia de cada característica considerada:

Cargos Fijos	***0,1***
Cargos Variables	***0,15***
Tipo de moneda a facturar	***0,05***
Idioma del soporte	***0,05***
Ubicación de las oficinas comerciales	***0,15***
Ubicación de los datacenters principales	***0,2***
Reputación en el mercado	***0,05***

Certificación de normas ISO	***0,1***
Planes de continuidad operativa	***0,1***
Disponibilidad operativa garantizada	***0,05***

Bibliografía

Bibliografía

AAIP. (19 de abril de 2020). *Agencia de Acceso a la Información Pública.* Obtenido de Disposición N° 11/2006: http://www.jus.gob.ar/datos-personales.aspx

Agencia Española de Protección de Datos. (15 de Octubre de 2017). *Guía para clientes que contraten servicios de Computing Cloud.* Obtenido de Agencia Nacional de Protección de Datos Personales de España: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf

Aldegani, G. (2019). “Compliance”. Exposición en la materia:. *Gestión Estratégica de la Seguridad Informática II.* Maestría en Seguridad Informática - UBA., Buenos Aires.

Arboledas Brihuega, D. (2014). *BackTrack 5.* México: Alfaomega Grupo Editor.

Argentina. (03 de Septiembre de 2017). *Congreso de la Nación Argentina. Ley N° 20.488. Artículo N° 13.* Obtenido de Ley de Incumbencias Profesionales en Ciencias Económicas. : www.infoleg.gov.ar

Barbei , A. A. (2017). *UTILIDAD DE LA INFORMACIÓN CONTABLE: MEJORAS A PARTIR DE LA FUNDAMENTACIÓN TEÓRICA DE LA MEDICIÓN Y LA EMISIÓN DE INFORMACIÓN .* Buenos Aires: Tesis Doctoral, Facultad de Ciencias Ecónómicas, UBA.

Bawaneh, S. S. (2022). Information Security for Organizations and Accounting Information Systems A Jordan Banking Sector Case. *International Review of Management and Business Research. Department of Accounting King Talal School for Business and Technology Princess Sumaya University for Technology*, Box 1438 Amman 11941 Jordan.

BCRA. (04 de Enero de 2006). *Comunicación "A" 4609: "Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información".* Buenos Aires: Banco Central de la República Argentina. Obtenido de Banco Central de la República Argentina: http://www.bcra.gov.ar/pdfs/comytexord/A4609.pdf

BCRA. (2012). *Comunicación “A” 5374: "Normas sobre “Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras”.* Buenos Aires: Banco Central de la República Argentina.

BCRA. (2016). *Comunicación “A” 6017, "Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras”.* Buenos Aires: Banco Central de República Argentina.

BCRA. (20 de enero de 2017). *Comunicación "A" 6354: “Expansión de entidades financieras” y “Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras”.* Buenos Aires: Banco Central de la República Argentina. Obtenido de http://www.bcra.gov.ar/: http://www.bcra.gov.ar/pdfs/comytexord/A6354.pdf

Biondi, M. (2012). Los Bienes intangibles y los intereses en los costos de producción analizados con enfoque en la contabilidad de gestión. *Contabilidad Y Auditoría*, 22.

Cano M., J. J. (2013). *Inseguridad de la Información. Una visión estratégica.* Bogotá: Alfaomega.

Cano M., J. J. (2015). *Computación Forense. Descubriendo los rastros informáticos* (Segunda ed.). México: Alfaomega.

Celeita, J. G. (02 de abril de 2020). *PROCESO DE SISTEMAS DE INFORMACION.* Obtenido de Municipio de Villavicencio, Colombia: http://www.villavicencio.gov.co/Transparencia/MECI%20Calidad/Instructivos%20Planes%20y%20Guias/Proceso%20De%20Sistemas%20De%20La%20Informacion/Instructivos/1152-I-SIF-09-

V2%20INSTRUCTIVO%20ALFABETIZACION%20DIGITAL%20A%20LA%20POBLACION%20DE%20VILLAVICENCIO.pdf

Chaves, O., Chyrikins, H., Dealecsandris, R., Pahlen Acuña, R., & Viegas, J. C. (1998). *Teoría Contable.* Buenos Aires: Ediciones Macchi.

Chiquiar, W. R. (2009). Aproximación a un marco conceptual de la contabilidad no monetaria (aplicada a la contabilidad ambiental). *Documentos de trabajo en Contabilidad Social. Aspectos particulares de Gestión Ambiental – las Empresas y sus Informes…*, 119-139.

Chiquiar, W. R. (2018). *Tesis Doctoral: LOS SISTEMAS DE INFORMACIÓN CONTABLE NO MONETARIOS (SIC-NM) Y SU FUNDAMENTACIÓN CONCEPTUAL EN EL MARCO DE LA TEORÍA CONTABLE.* Buenos Aires: Facultad de Ciencias Económicas, Universidad de Buenos Aires.

CitiGroup. (2018). *Modelo de Evaluación de la Seguridad de la Información de Citigroup.* Buenos Aires: Grupo Citibank.

CODECE. (03 de diciembre de 2019). *Consejo de Decanos de Facultades de Ciencias Económicas de Universidades Nacionales.* Obtenido de http://www.codece.com.ar/docs/Estatuto01072011.pdf

Comisión Nacional de Valores. (22 de enero de 2020). *CNV.* Obtenido de Sitio de la CNV: http://www.cnv.gob.ar/leyesyreg/cnv/esp/rgcrgn629-14.htm

Committee of Sponsoring Organizations of the Tread. (2013). *Internal Control – Integraded Framework.* Edición digital.

Congreso de la Nación Argentina. (2014). *Código Civil y Comercial, Artículo N° 322.* Buenos Aires: República Argentina.

Congreso de la Nación Argentina. (2014). *Código Civil y Comercial, Artículo N° 329, Actos sujetos a autorización.* Buenos Aires: República Argentina.

Congreso de la República Argentina. (19 de abril de 2020). *Ley N°25.326*. Obtenido de Infoleg: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

CXO Media Inc. (01 de Octubre de 2019). *CERT Security Capability Assessment Tool.* Obtenido de Carnegie Melon University: www.csoonline.com/surveys/securitycapability.html

Escobar, D. S. (2010). Ley de Protección de Datos Personales. *Revista Imagen Profesional de La Federación Argentina de Consejos Profesionales en Ciencias Económicas*, 22-24.

Escobar, D. S. (2013). *SEGURIDAD INFORMÁTICA EN LOS SISTEMAS CONTABLES: Un análisis de los aspectos legales, normativos y tecnológicos de la Seguridad de la Información en el almacenamiento, procesamiento, control y resguardo de los Registros Contables.* Buenos Aires: Facultad de Ciencias Económicas. UBA.

Escobar, D. S. (2017). Concientización y capacitación del educando en la criticidad de la información contable en el ámbito de la práctica profesional. *XXXIX SIMPOSIO DE PROFESORES DE PRÁCTICA PROFESIONAL* (págs. 40-50). San Fernando del Valle de Catamarca: UNIVERSIDAD NACIONAL DE CATAMARCA.

FACPCE. (2011). *Marco Conceptual - Resolución Técnica 16.* Buenos Aires: Federación Argentina de Consejos Profesionales en Ciencias Económicas, Marco Conceptual - RT 16. República Argentina, 2011.

Federación Argentina de Consejos Profesionales de Ciencias Económicas. (2008). *RT N° 16: Marco Conceptual de las Normas Contables Profesionales.* Buenos Aires: FACPCE.

Fowler Newton, E. (2020). *Cuestiones Contables Fundamentales.* Buenos Aires: La Ley.

Fronti de García, L., & García Casella, C. (2009). *El sistema contable de gestión ambiental ante el cambio climático.* Buenos Aires: Universidad de Buenos Aires.

García Casella, C. (1992). *Corrientes doctrinarias actuales en contabilidad.* Buenos Aires: Facultad de Ciencias Económicas, Universidad de Buenos Aires.

García Casella, C. (1997). Naturaleza de la Contabilidad. *Revista "Contabilidad y Auditoría" Año 3 N° 5*, 12-37.

García Casella, C. (2002). El problema del uso de modelos en la contabilidad. *Revista Legis Internacional de Contabilidad y Auditoría*, 199-236.

García Casella, C. L. (1995). Método Científico para las Investigaciones en General. *1er Encuentro Universitario de Investigaciones del Área Contable.* Buenos Aires: UBA.

García Casella, C. L. (2001). Elementos para una teoría general de la contabilidad. En C. L. García Casella, & M. d. Rodriguez de Ramirez. Buenos Aires: La Ley.

García Casella, C. L. (2001). Elementos para una teoría general de la contabilidad. En C. L. García Casella. Buenos Aires: La Ley.

García Casella, C. L., & Rodríguez de Ramírez, M. (2011). Elementos para una Teoría General de la Contabilidad. En C. L. García Casella, & M. d. Rodríguez de Ramírez, *[Traducción de: American Accounting Association, 1966, "A Statement of Basic Accounting Theory".* Buenos Aires: La Ley.

García Casella, C. L., Fronti de García, L., & Rodríguez de Ramírez, M. (2001). *Elementos para una teoría general de la contabilidad.* Buenos Aires: La Ley.

Gómez López, J. (2010). Seguridad Informática. En G. L. J., *Guía de campo de Seguridad Informática* (pág. 17). México: Alfaomega Grupo Editor.

Henry, L. (2020). A study of the nature and security of accounting information systems: The case of Hamptom Roads, Virginia. *Old Dominion university, Departament of Accounting*, 229.

IASB. (2007). *Marco Conceptual para la Preparación y Presentación de Estados Financieros.* Buenos Aires: FACPCE.

Information Systems Audit and Control Association. (06 de Septiembre de 2019). *Objetivos de Control para Información y Tecnologías Relacionadas.* Obtenido de (COBIT 5, Control Objectives for Information and related

Technology). ISACA (Information Systems Audit and Control Association): www.itgi.org

Inspección General de Justicia. (08 de enero de 2020). *IGJ.* Obtenido de Resolución General N° 7 de 2015. Artículo N° 334. Boletín Oficial de la República Argentina.: www.infoleg.gov.ar

Instituto de Auditores Internos de Argentina. (06 de Septiembre de 2019). *Boletín de la Comisión de Normas y Asuntos Profesionales" Nº 9.* Obtenido de IAIA: https://www.iaia.org.ar/revistas/normaria/Normaria09.pdf

International Accounting Standards Board, (. d. (07 de Septiembre de 2017). *El Marco Conceptual para la Información Financiera.* Obtenido de International Financial Reporting Standards: http://www.ifrs.org/

International Accounting Standards Board, (. d. (07 de enero de 2020). *El Marco Conceptual para la Información Financiera.* Obtenido de International Financial Reporting Standards: http://www.ifrs.org/

International Organization for Standardization / International Electrotechnical Commission. (2013). *27002.* Suiza: ISO.

International Organization for Standardization. (2015). *ISO 9001 Sistemas de Gestión de Calidad.* Inglaterra: International Organization for Standardization.

IRAM/ISO/IEC. (2018). *ISO/IEC 27.001 Information technology - Security techniques - Information security management systems - Requirements.*

Inglaterra: International Organization for Standardization - International Electrotechnical Commission.

ISACA. (2010). *The Business Model for Information Security (BMIS).* Estados Unidos: Information Systems Audit and Control Association.

Jasim, Y., & Raewf, M. (2022). Impact of the Information Technology on the Accounting System. *Journals Cihan University. Department of Accounting, Cihan University-Erbil, Kurdistan Region*, 1-32.

Kahate, A. (2019). *Cryptography and network security.* Chennai: McGraw Hill Education.

Katz, M. (2013). *Redes y seguridad.* México: Alfaomega.

Kaufmann, A., & Gil-Aluja, J. (1991). *Introducción de la teoría de los subconjuntos borrosos a la gestión de las empresas.* Barcelona: Facultad de ciencias económicas y empresariales.

Lazzari, L. L., Marachado, E., & Perez, R. (1998). *Matemática Borrosa, Técnicas de Gestión para el tratamiento de la incertidumbre. .* Universidad de Buenos Aires: Facultad de Ciencias Económicas.

Lazzari, L. L., Moulia, P., & Fogel, A. J. (2012). AGRUPACIÓN DE PRODUCTOS FINANCIEROS POR AFINIDAD. *CIMBAGE – IADCOM, Facultad de Ciencias Económicas, Universidad de Buenos Aires.*

López, P., Moya, F., Marimón, S., & Planas, I. (2011). *Protección de datos de salud. Criterios y plan de seguridad.* Madrid: Diaz de Santos.

Malimage, K., Raddatz, N., Trinkle, B. S., & Crossler, R. E. (2020). Impact of Deterrence and Inertia on Information Security Policy Changes. *Journal of Information Systems, American Accounting Association*, 123–134.

Mattessich, R. (1964). *Accounting and analytical methods. Measurement and projection of income and wealth in the micro- and macro-economy.* Homewood, Illinois: Richard D. Irwin, Inc. .

Mattessich, R. (2002). *Contabilidad y Métodos Analíticos. Medición y proyección del ingreso y la riqueza en la microeconomía y macroeconomía.* Buenos Aires: Editorial La Ley.

Mejía Soto, E., Montes Salazar, C., & Dávila, G. (2011). Introducción a la propuesta contable de García-Casella. *Cuadernos de Contabilidad, 12 (30)*, 127-164.

Mejía-Soto, E., & Montes-Salazar, C. A. (2011). Introducción a la propuesta contable de García-Casella. *Cuadernos de Contabilidad*, 127-164.

Mouliá, P., & Lazzari, L. L. (2012). APLICACIÓN DE LOS CONJUNTOS BORROSOS A LA MEDICINA PREPAGA. *CIMBAGE – IADCOM, Facultad de Ciencias Económicas, Universidad de Buenos Aires*.

National Institute of Standards and Technology. (10 de Octubre de 2019). *NIST SP 800-12 - An Introduction to Computer. Security: The NIST Handbook.* Obtenido de National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

ONTI. (19 de Abril de 2020). *Modelo de Política de Seguridad de la Información.* Obtenido de www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf

Peso Navarro, E. d., Ramos, M. A., & Peso, M. d. (2004). *El documento de Seguridad (Análisis Técnico y Jurídico. Modelo).* Madrid: Diaz de Santos.

Petratos, P., & Faccia, A. (2019). Accounting Information Systems and System of Systems: Assessing Security with Attack Surface Methodology. *ICCBDC 2019: Proceedings of the 2019 3rd International Conference on Cloud and Big Data Computing*, 100–105.

Portantier, F. (2013). *Gestión de la Seguridad Informática.* Buenos Aires: Fox Andina en coedición con DÁLAGA SA.

Portantier, F. (2019). *Seguridad Informática.* Buenos Aires: Fox Andina Dálaga.

Qayssar, A.-F., Dawood, S., & Akeel, H. (02 de 05 de 2022). *Accounting Information Security and IT Governance Under COBIT 5 Framework: A Case Study.* Obtenido de Faculty of Administration and Economics, University of Kufa: https://www.webology.org/data-cms/articles/20210429122040pmWEB18073.pdf

RAE. (10 de Octubre de 2017). *Real Academia Española*. Obtenido de Seguro/ra [en línea]: http://lema.rae.es/drae/?val=Seguro

Ramírez, M. (2017). *Métricas de seguridad.* Buenos Aires: COA S.A.

Ramírez, M. d., & Marcolini, S. (2013). *SUBORDINACION, COOPERACION Y COORDINACION ENTRE EMPRESAS: RELACIONES PARA GENERAR INFORMACION CONTABLE.* Rosario: SaberEs.

Real Academia Española. (09 de septiembre de 2017). *Real Academia Española*. Obtenido de Definición de dato: http://dle.rae.es/?id=Bskzsq5|BsnXzV1

Real Academia Española. (09 de abril de 2020). *Real Academia Española*. Obtenido de Definición de dato: http://dle.rae.es/?id=Bskzsq5|BsnXzV1

Sallis, E., Caracciolo, C., & Rodriguez, M. (2010). *Ethical Hacking - Un enfoque metodológico para profesionales.* Buenos Aires: Alfaomega Grupo Editor.

Saroka, R. (17 de abril de 2020). *Sistema de Información.* Obtenido de Biblioteca de la Funcación OSDE: http://www.fundacionosde.com.ar/pdf/biblioteca/Sistemas_de_informacion_en_la_era_digital-Modulo_I.pdf

Scolnik, H. D. (2014). *Qué es la Seguridad Informática.* Buenos Aires: Paidós.

Senge, P. (1992). *La Quinta Disciplina.* Barcelona: Granica.

Senge, P., Ross, R., Smith, B., Roberts, C., & Kleiner, A. (2004). *La Quinta Disciplina en la Práctica.* Buenos Aires: Granica.

Shaw, T. (2011). *SHAW, T. (2011) Information security and privacy. A practical guide for global executives, lawyers and technologists.* ABA Section of Science & Technology.: American Bar Association.

Stallings, W. (2016). *Cryptography and Network Security. Principles and practice.* Londres: Pearson Prentice Hall.

Steinbart, P., Raschke, R., Gal, G., & Dilla, W. (2021). Information Security Professionals' Perceptions about the Relationship between the Information Security and Internal Audit Functions. *Journal of Information Systems American Accounting Association*, 65–86. Obtenido de Journal of Information Systems Journal of Information Systems .

Suarez Kimura, E. B., & Escobar, D. E. (2017). Identificación de conceptos básicos de la ley de habeas data en los sistemas contables: perspectivas a considerar por parte de los pequeños estudios. *Enfoques*, 40-56.

Suarez Kimura, E. B., & Escobar, D. S. (2010). Repercusiones de La Ley De Protección de Datos Personales en el Ejercicio Profesional del Contador Público. *Foro Nacional de Simposios de Profesores de Práctica Profesional*, Publicación contínua.

Tesoro, J. (1998). *Estado de la Cultura Informativa.* Bahía Blanca: Universidad Nacional del Sur.

The International Systems Security Engineering Association (ISSEA). (20 de octubre de 2019). *SSE-CMM - Systems Security Engineering Capability Maturity Model.* Obtenido de Carnegie Melon University: www.ssecmm.org

Tipton, H., & Krause, M. (2005). Information Security Management Handbook. En H. Tipton, & M. Krause, *Social Science, Psychology, and Security Awareness: Why?* Editorial AUERBACH.

Tipton, H., & Krause, M. (2005). Attitude Structure and Function: The ABC's of the Tripartite Model. En H. Tipton, & M. Krause, *Information Security Management Handbook.* Editorial AUERBACH.

Ugalde Binda, N. (2019). Capital intelectual del emprendedor y la innovación. *Contabilidad Y Auditoría*, Recuperado a partir de http://ojs.econ.uba.ar/index.php/Contyaudit/article/view/1339.

Vázquez, R., & Bongianino de Salgado, C. (2002). *Los activos intangibles y la contabilidad.* Buenos Aires: ERREPAR.

Vicente, A. (11 de Noviembre de 2019). *ISM3: Nuevo estándar para la gestión de la seguridad de la información.* Obtenido de http://www.kriptopolis.org/ism3-nuevo-estandar-para-la-gestion-de-la-seguridad-de-la-informacion

Villegas, M. (2008). Modelo de Madurez para la Gestión y Administración de la Seguridad Informática en las Universidades. *Trabajo de Grado para optar a la Magíster en Ingeniería de Sistemas*. Caracas, Venezuela: Universidad Simón Bolívar.

Villegas, M., Orlando, V., & Walter, B. (2009). Modelo de Madurez de la Gestión de la Seguridad Informática en el Contexto de las Organizacion es Inteligentes. *Seventh LACCEI Latin American and Caribbean Conference for Engineering and Technology, Energy and Technology for the Americas: Education, Innovation, Technology and Practice.* Venezuela: LACCEI.

Wang, Y. (2021). Research on Security of Accounting Information System in the Era of Big Data. *Journal of Physics: Conference Series, Volume 1881, The 2nd International Conference on Computing and Data Science (CONF-CDS) 2021 28-30 January 2021, Stanford, United States*, Conf. Ser. 1881 042030.

WordPress. (09 de septiembre de 2017). *Página de definiciones del lenguaje castellano*. Obtenido de https://definicion.de/: https://definicion.de/informacion/

- Bibliografía general

Agencia Nacional de Promoción Científica y Tecnológica. “Fondo para la Investigación Científica y Tecnológica” diciembre de 2015. Accedido desde http://www.agencia.mincyt.gob.ar/frontend/agencia/fondo/foncyt

Agencia Española de Protección de Datos. (2013). Guía para clientes que contraten servicios de Computing Cloud.

Aldegani G. (2011), “Compliance”. Exposición en la materia: “Gestión Estratégica de la Seguridad Informática II”. 18 de julio de 2011. Maestría en Seguridad Informática. Buenos Aires.

American Accounting Association. (1966), “A Statement of Basic Accounting Theory”, AAA.

Asociación Interamericana de Contabilidad. (2013), XXX Conferencia Interamericana de Contabilidad, Uruguay 2013. “Conclusión y recomendaciones”, Área 9 – Sistemas y Tecnología de la Información. Accedido de http://www.contadores-aic.org/

Bermúdez José D., Segura José V., Vercher Enriqueta. (2009), Modelos borrosos de optimización para la selección de carteras basados en intervalos de medias / Optimization Fuzzy Models for the Selection of Portfolios Based on Media Intervals. Cuaderno N°9. Facultad de Ciencias Económicas. Universidad de Buenos Aires.

Brihuega Arboledas, D. (2014), “BackTrack 5, Hacking de Redes inalámbricas.” Alfaomega Ra-Ma, México.

Burgos, A. (2009), “Seguridad, Proteja sus datos y privacidad”, Editorial Users, Buenos Aires.

Cano Martinez, J. (2009), “Computación Forense, descubriendo los rastros informáticos”; Alfaomega Ra-Ma, México.

Carrizo, M.A., Casparri, M.T. y Taboada, E. "Una selección de canales de distribución a través de relaciones borrosas" Cuaderno Nº3, Aplicaciones de metodologías borrosas a temas de gestión y economía. Facultad de Ciencias Económicas, Buenos Aires, marzo de 2000. ISBN 950-29-0562-8. Director de la colección: Emilio A. M. Machado.

Chalupowicz, D. G. (2006), “Responsabilidad Corporativa, informe COSO: la ley Sarbanes Oxley. Auditoría Interna y externa.” 2da. Edición. Buenos Aires.

Committee of Sponsoring Organizations of the Treadway Commission – COSO. (2013), “Internal Control – Integrated Framework”. Edición digital - Mayo 2013.

Congreso de la Nación Argentina, “Código Civil y Comercial”, Sección 7ª, Contabilidad y estados contables. Accedido desde www.infoleg.gov.ar el 10 de diciembre de 2015.

Congreso de la Nación Argentina, “Ley N°19950, Ley General de Sociedades”, Artículo N° 61, Boletín Oficial de la República Argentina, agosto de 2015, Buenos Aires.

Congreso de la Nación Argentina. (2014), Código Civil y Comercial.

Congreso de la Nación Argentina. “Ley N° 20.488. Ley de Incumbencias Profesionales en Ciencias Económicas.” Accedido desde www.infoleg.gov.ar el 10 de diciembre de 2015.

Consejo de Decanos de Facultades de Ciencias Económicas de Universidades Nacionales. “Estatuto” diciembre de 2015. Accedido desde http://www.codece.com.ar/docs/Estatuto01072011.pdf

Dirección Nacional de Protección de Datos Personales. (2006), “Disposición N° 11/2006, Medidas de Seguridad”. Buenos Aires, Argentina., accedido desde http://www.jus.gob.ar/datos-personales.aspx

Dubois E. M. F., “La Contabilidad Informática ¿Brinda Seguridad Jurídica en su actual implementación?”, Revista Errepar [en línea]. Julio de 2001.

[consultada el 20 de agosto de 2011]. Disponible en: http://www.legalmania.com.ar/derecho/contabilidad_informatica.htm

Escobar, D. S. (2010), “Aportes de la Ley de Protección de datos personales en el Sistema de Información Contable. Nuevos conocimientos del Contador Público en la era de la información.” 18º Congreso Nacional de Profesionales en Ciencias Económicas”, Ciudad Autónoma de Buenos Aires.

Escobar, D. S. (2010), “Ley de Protección de Datos Personales, Revista Imagen Profesional”, de La Federación Argentina de Consejos Profesionales en Ciencias Económicas. Buenos Aires.

Escobar, D. S. (2013) Seguridad informática en los sistemas contables: un análisis de los aspectos legales, normativos y tecnológicos de la seguridad de la información en el almacenamiento, procesamiento, control y resguardo de los registros contables. Facultad de Ciencias Económicas. Universidad de Buenos Aires.

Escobar, D. S. (2014), “El Sistema de Gestión de Seguridad de la Información y las incumbencias profesionales del Contador Público.” Área: Actualización de contenidos programáticos. XXXV Simposio Nacional de Profesores de Práctica Profesional. Concordia.

Escobar, D. S. (2014), “Gestión de mejoras prácticas y estándares de control y tecnologías en los sistemas contables”, Asociación Interamericana de Contabilidad”, octubre 2014.Comisión Técnica de Sistemas y Tecnologías de Información, Charla Cibernética.

Escobar, D. S. (2014), “Implicancias legales de la Firma Digital y Electrónica en el resguardo de documentación respaldatoria y registros contables.” Presentado en la VII JORNADA NACIONAL DE DERECHO CONTABLE, junio de 2014, Consejo Profesional de Ciencias Económicas de Santa Fe, Ciudad de Rosario.

Escobar, D. S. y otros. “Aspectos legales y formales del sistema de registro “Legal Forma”, Comisión de Estudios sobre Sistemas de Registros, su integridad y autenticidad documental, Informe 1, EDICION, Buenos Aires.

Escobar, D. S., Ley de Protección de Datos Personales, Revista Imagen Profesional, de La Federación Argentina de Consejos Profesionales en Ciencias Económicas, 2010.

Federación Argentina de Consejos Profesionales en Ciencias Económicas. (2011), Marco Conceptual - RT 16. República Argentina.

Federación Internacional de Contadores (IFAC), “Formas Internacionales de Formación”; 2008, [consultada el 10 de noviembre de 2015]. Disponible en: “http://www.ifac.org/sites/default/files/downloads/Spanish_Translation _Normas _Internacionales_de_ Formacion_2008.pdf”

Fowler Newton, E. (1982), “Organización de Sistemas Contables”. Ediciones Contabilidad Moderna. Buenos Aires.

Fowler Newton, E. (2009), “Planes de Cuentas y Manuales de Procedimientos Contables”. Editorial La Ley, Buenos Aires.

Fronti de García, L. (1968), “La Formación del Contador Público en la UBA”, Tesis Doctoral. Facultad de Ciencias Económicas, Universidad de Buenos Aires.

García Casella C. L. y Rodríguez de Ramírez M. C. (2001), “Elementos para una Teoría General de la Contabilidad”, Buenos Aires.

García Casella, C. L. (1995), “Método Científico para las Investigaciones en General”, Informe presentado en el 1er Encuentro Universitario de Investigaciones del Área Contable, Buenos Aires.

Gómez López J. (2010), “Guía de campo de hackers”, Alfaomega Grupo Editor, México.

Gómez López, J. y otros. (2010), “Administración Avanzada de los sistemas informáticos”; Alfaomega Ra-Ma, México.

Gómez Vieites, Á. (2011), “Enciclopedia de la Seguridad Informática”, 2da edición. Alfaomega Ra-Ma, México.

Inspección General de Justicia. (2015), “Resolución General N° 7 de 2015”. Boletín Oficial de la República Argentina, 23 de agosto de 2015.

Instituto Autónomo de Derecho Contable, IADECO. (2011), “Nuevos Aportes al Derecho Contable”, Libro de Ponencias, Editorial Errepar, Buenos Aires.

International Auditing Practices Committee (of the International Federation of Accountants). (2001), “Electronic Commerce Using the Internet or Other Public Networks – Effect on the Audit of Financial Statements”. Exposure Draft. New.

International Organization for Standardization - International Electrotechnical Commission. (2013), “ISO/IEC 27.001 Information technology - Security techniques - Information security management systems – Requirements”. Edición Digital.

International Organization for Standardization - International Electrotechnical Commission. (2005), “ISO/IEC 20.001 Gestión de servicios de TI” (Tecnologías de la Información). Edición Digital.

International Organization for Standardization (2008), “ISO 9001 Sets out the requirements of a quality management system”. Edición Digital.

IT Governance Institute, (2013), “Objetivos de Control para Información y Tecnologías Relacionadas” (COBIT 5, Control Objectives for Information and related Technology). ISACA (Information Systems Audit and Control Association). Accedido desde www.itgi.org

Jaime Gil L. “Nuevo instrumento de selección: el “índice de descartes por superación-distancia” / A New Instrument for Selection: the “Index of Elimination by Excess-Distance”. Cuaderno N°7. Facultad de Ciencias Económicas. Universidad de Buenos Aires.

Katz, Matías; (2013), “Redes y Seguridad”, Aflaomega, México.

Kaufmann A., Gil-Aluja J. (1991), Introducción de la teoría de los subconjuntos borrosos a la gestión de las empresas. Facultad de ciencias económicas y empresariales, Barcelona.

Laudon, K, y Laudon, J. (2012), "Sistemas de Información Gerencial", Editorial. Prentice Hall, Hispanoamericana, México.

Lazzari Luisa L. (2010) “El comportamiento del consumidor desde una perspectiva fuzzy: una aplicación al turismo”. Editor: EDICON. Buenos Aires.

Lazzari Luisa L., Machado Emilio, Pérez Rodolfo. (1998) "Un problema de selección del personal". Cuaderno Nº 1, “Aplicaciones de metodologías borrosas a temas de gestión y economía.” Director de la colección: Emilio A. M. Machado. Editores: Luisa L. Lazzari, Emilio A. M. Machado y Rodolfo H. Pérez. Facultad de Ciencias Económicas, Buenos Aires.

Lazzari Luisa L., Moulia Patricia, Fogel Aquilante Jennifer, (2012), “AGRUPACIÓN DE PRODUCTOS FINANCIEROS POR AFINIDAD”. CIMBAGE – IADCOM, Facultad de Ciencias Económicas, Universidad de Buenos Aires. www.econ.uba.ar/cimbage

Ley N° 19950, Ley General de Sociedades, Boletín Oficial de la República Argentina Buenos Aires, 2015.

Ley N° 25326, Ley de Habeas Data, Boletín oficial de la República Argentina, Buenos Aires. 30 de octubre de 2000.

Marshall B., Romney, y P, Steinbart J. (2012), “Accounting Information Systems”, 12th Edition, New Jersey.

Molina, J. C., (1999), “Los subdiarios y la obligatoriedad de su rubricación, Impuestos”, LVII-1999-A, Ed. La Ley, p. 1550. Buenos Aires.

Mouliá Patricia, Lazzari Luisa L., (2012), “APLICACIÓN DE LOS CONJUNTOS BORROSOS A LA MEDICINA PREPAGA”. CIMBAGE – IADCOM, Facultad de Ciencias Económicas, Universidad de Buenos Aires. www.econ.uba.ar/cimbage

Pastor J. S., Bessana G. A. e Iglesias S. G. (2010), “Procedimiento General para la Emisión, Conversión y Conservación de la documentación respaldatoria en los sistemas de registros contables. Aspectos legales y técnicos”. En: 18° Congreso Nacional de Profesionales en Ciencias Económicas: (18, 2010, CABA), Área V. Administración y Sistemas. Buenos Aires.

Paulino E. Mallo; Maria A. Artola; Alicia I. Zanfrillo; Mariano Morettini; Marcelo J. Galante; Mariano E. Pascual, Adrián R. Busetto. “Una propuesta de selección de entidades aseguradoras a partir de un modelo de lógica compensatoria difusa / Proposal for selection of insurance companies based on a compensatory fuzzy logic model”. Cuaderno N°12. Facultad de Ciencias Económicas. Universidad de Buenos Aires. ISSN 1666-5112 (versión impresa) ISSN 1669-1830 (versión en línea).

Popritkin A. R. (2001), Fraudes y Libros Contables, La Ley, Buenos Aires.

Portantier, F. (2012), “Seguridad Informática”, RedUsers. Buenos Aires.

Sallis E., Caracciolo C., y Rodríguez M. (2010), “Ethical Hacking, Un enfoque metodológico para profesionales”, Editorial Alfaomega. Buenos Aires.

Saroka R. (2002), “Sistemas de Información en la era de digital”, Fundación Osde. Buenos Aires.

Scolnik, H. (2014), “¿Qué es la seguridad informática?”, Editorial PAIDOS, Buenos Aires.

Security Standards Council LLC. (2013), (PCI-DSS) “Normas de seguridad de datos, Requisitos y procedimientos de evaluación de seguridad”, Industria de Tarjetas de Pago (PCI), Versión 3, accedido desde www.pcisecuritystandards.org

Sosa, T. E., (1999), “Medios informáticos y el proceso que viene. Validez probatoria y eficiencia procesal”. La Ley, Buenos Aires.

Spina, C. E. (2008), “Factura Electrónica”, 2 edición, Osmar D. Buyatti Librería Editorial, Buenos Aires.

Stallings, W. (2010), “Cryptography and Security Network, Principles and Practices”, Pearson Education.

Suarez Kimura E. B. y Escobar, D. S. (2010), “Repercusiones de La Ley De Protección de Datos Personales en el Ejercicio Profesional del Contador Público”, en el XXXII Simposio Nacional de Profesores de Práctica Profesional del Contador. Facultad de Humanidades, Ciencias Sociales y de la Salud, Universidad Nacional de Santiago del Estero.

Suarez Kimura Elsa B. (2004). “Auditoría y Sistema de Control Interno: Particularidades a considerar en los contextos tecnológicamente mediados”. XXVI Simposio de Profesores de Práctica Profesional. Universidad del Museo Social Argentino. Buenos Aires.

Suarez Kimura Elsa B. (2008), “Tesis Doctoral, Posibles mejoras teórico-tecnológicas aportadas por la contabilidad a los Sistemas de información de los entes”. Investigación y Doctorado, Facultad de Ciencias Económicas, Universidad de Buenos Aires.

Suarez Kimura, E. B. (2004), Auditoría y Sistema de Control Interno: Particularidades a considerar en los contextos tecnológicamente mediados. XXVI Simposio de Profesores de Práctica Profesional. Universidad del Museo Social Argentino. Buenos Aires.

Suarez Kimura, E. B. (2008), “Tesis Doctoral, Posibles mejoras teórico-tecnológicas aportadas por la contabilidad a los Sistemas de información de los entes”. Investigación y Doctorado, FCE UBA. Buenos Aires.

Suarez Kimura, E. B., Escobar, D. S. y De Franceschi, R. L. (2014), “El rol del profesional en Ciencias Económicas en la planificación estratégica de las tecnologías de información.”. XXXVI Simposio Nacional de Profesores de Práctica Profesional. Faculta de Ciencias Económicas, UADE. Pinamar.

Universidad de Buenos Aires. “Programación Científica UBACYT 2014/2017” diciembre de 2015. Accedido desde http://secinves.com.ar/guias/ubacyt

Universidad Notarial Argentina, Instituto de Derecho Comercial, (2000), “Condiciones de la legalidad de la contabilidad informática”, Conclusiones generales. Buenos Aires.

- Índices específicos

- Notas

[i] Traducción de: “The banking sector typically needs the most improvement of tech and is more inclined to opt to outsource in the face of such circumstances. Development of corporate applications accounts for 50% of the IT budget managed and outsourced in most cases (De la Fuente Asprón, 2010). However, some banks do not measure software and maintenance, despite being one of the most extensive IT processes.” (Qayssar, Dawood, & Akeel, 2022)

[ii] Traducción de: “We also find that the quality of the relationship between the internal audit and information security functions is positively associated with perceptions about the value provided by internal audit and, most important, with measures of overall effectiveness of the organization's information security endeavors. (Steinbart, Raschke, Gal, & Dilla, 2021)

[iii] Traducción de “The employment of information technology mechanisms in the AIS contributed to reducing unintended errors and thus contributed to the development of the auditing profession. The efficient application of information technologies contributed to the flow of information effectively, which facilitated the taking of management decisions, and improved the company’s ability to meet strategic and commercial goals.” (Jasim & Raewf, 2022)

[iv] Traducción de: “This research examines three types of information security and control procedures for organizations that are expected to be used within Accounting Information Systems (AIS): security and general control for organizations; security and general control for Information Technology (IT), and application controls for transaction processing.” (Bawaneh, 2022)

[v] Traducción de “Further, more and more articles are appearing in these publications discussing security methods for the new technologies.” (Henry, 2020)

[vi] Traducción de: “At the same time there is an increasingly cyber security risk for AIS, which can be considered part of critical infrastructure, in that sense assessing cybersecurity risks is essential.”

(Petratos & Faccia, 2019)

[vii] Traducción de: “Therefore, organizations must work to overcome employees' reluctance to change in order to improve compliance with security policy modifications.” (Malimage, Raddatz, Trinkle, & Crossler, 2020)

[viii] Dado que la titularidad legal de ciertos datos existentes en las compañías corresponde a sus clientes, la entidad tiene la custodia de esta.

[ix] El conjunto de componentes de hardware, conectados físicamente mediante cables u ondas, y configurados de una manera homogénea y sincronizada, que permiten establecer comunicaciones entre sí. (Katz, 2013)

[x] *“Security Services (X.800)*

1. AUTHENTICATION: The assurance that the communicating entity is the one that it laims to be. Peer Entity Authentication: Used in association with a logical connection to provide confidence in the identity of the entities connected. Data Origin Authentication: In a connectionless transfer, provides assurance that the source of received data is as claimed.

2. ACCESS CONTROL: The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

3. DATA CONFIDENTIALITY: The protection of data from unauthorized disclosure. Connection Confidentiality: The protection of all user data on a connection.

Connectionless Confidentiality: The protection of all user data in a single data block Selective-Field Confidentiality: The confidentiality of selected fields within the user Data on a connection or in a single data block. Traffic Flow Confidentiality: The protection of the information that might be Derived from observation of traffic flows.

4. DATA INTEGRITY: The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay). Connection Integrity with Recovery: Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted. Connection Integrity without Recovery: As above but provides only detection without recovery. Selective-Field Connection Integrity: Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed. Connectionless Integrity: Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided. Selective-Field Connectionless Integrity: Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

5. NONREPUDIATION: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. Nonrepudiation, Origin: Proof that the message was sent by the

specified party. Nonrepudiation, Destination: Proof that the message was received by the specified party." (Kahate, 2019)

[xi] En el punto 3.1.4.1. de la Comunicación "A" 4609 del BCRA.

[xii] Se requerirá título de Contador Público o equivalente:

a) En materia económica y contable cuando los dictámenes sirvan a fines judiciales, administrativos o estén destinados a hacer fe pública en relación con las cuestiones siguientes:

1. Preparación, análisis y proyección de estados contables, presupuestarios, de costos y de impuestos en empresas y otros entes.

2. Revisión de contabilidades y su documentación.

3. Disposiciones del Capítulo III, Título II, Libro I del Código de Comercio.

4. Organización contable de todo tipo de entes.

5. Elaboración e implantación de políticas, sistemas, métodos y procedimientos de trabajo administrativo–contable.

6. Aplicación e implantación de sistemas de procesamiento de datos y otros métodos en los aspectos contables y financieros del proceso de información gerencial.

7. Liquidación de averías.

8. Dirección del relevamiento de inventarios que sirvan de base para la transferencia de negocios, para la constitución, fusión, escisión, disolución y liquidación de cualquier clase de entes y cesiones de cuotas sociales.

9. Intervención en las operaciones de transferencia de fondos de comercio, de acuerdo con las disposiciones de la Ley N° 11.867, a cuyo fin deberán realizar todas las gestiones que fueren menester para su objeto, inclusive hacer publicar los edictos pertinentes en el Boletín Oficial, sin perjuicio de las funciones y facultades reservadas a otros profesionales en la mencionada norma legal.

10. Intervención juntamente con letrados en los contratos y estatutos de toda clase de sociedades civiles y comerciales cuando se planteen cuestiones de carácter financiero, económico, impositivo y contable.

11. Presentación con su firma de estados contables de bancos nacionales, provinciales, municipales, mixtos y particulares, de toda empresa, sociedad o institución pública, mixta o privada y de todo tipo de ente con patrimonio diferenciado.

En especial para las entidades financieras comprendidas en la Ley N° 18.061, cada Contador Público no podrá suscribir el balance de más de una entidad cumplimentándose asimismo el requisito expresado en el Art. N° 17 de esta Ley.

12. Toda otra cuestión en materia económica, financiera y contable con referencia a las funciones que le son propias de acuerdo con el presente artículo.

b) En materia judicial para la producción y firma de dictámenes relacionados con las siguientes cuestiones:

1. En los concursos de la Ley N° 19.551 para las funciones de síndico.

2. En las liquidaciones de averías y siniestros y en las cuestiones relacionadas con los transportes en general para realizar los cálculos y distribución correspondientes.

3. Para los estados de cuenta en las disoluciones, liquidaciones y todas las cuestiones patrimoniales de sociedades civiles y comerciales y las rendiciones de cuenta de administración de bienes.

4. En las compulsas o peritajes sobre libros, documentos y demás elementos concurrentes a la dilucidación de cuestiones de contabilidad y relacionadas con el comercio en general, sus prácticas, usos y costumbres.

5. Para dictámenes e informes contables en las administraciones e intervenciones judiciales.

6. En los juicios sucesorios para realizar y suscribir las cuentas particionarias juntamente con el letrado que intervenga.

7. Como perito en su materia en todos los fueros.

En la emisión de dictámenes, se deberán aplicar las normas de auditoría aprobadas por los organismos profesionales cuando ello sea pertinente.

[xiii] Comisión de Sistemas de Registros, Integridad y Autenticidad documental. Consejo Profesional en Ciencias Económicas de la Ciudad Autónoma de Buenos Aires.

[xiv] En el plexo normativo de la IGJ se especifican los siguientes medios de almacenamientos: compact disc, otros discos ópticos y microfilmes, o similares.

[xv] Por lo tanto, hay que considerar la generación que permite leerlos.

[xvi] Sistemas de registración contable en compact disc, otros discos ópticos y microfilmes.

[xvii] Traducción de Social Science, Psychology, and Security Awareness: Why? Fuente: Tipton H. y Krause M. (2005).

[xviii] Traducción de “Attitude Structure and Function: The ABC's of the Tripartite Model”, Tipton H. y Krause M. (2005).

[xix] Traducido de: *1. Affect.* The affective component is the emotional aspect of our attitudes. Our feelings toward an object or subject play an important role in determining our attitudes. We are more likely to participate and do things that make us feel happy or good. Our aversion to things that elicit feelings of guilt, pain, fear, or grief can be used to change attitudes and, eventually, behavior. Fuente: Tipton H. y Krause M. (2005).

[xx] Traducido de: *2. Behavior.* The behavior component is derived from the fact that our behavior serves as a feedback mechanism for our attitudes. In short, "doing" leads to "liking." In an ingenious experiment, two randomly selected groups of subjects were asked to rate how much they liked a cartoon they were watching. The two groups watched the same cartoon, with only one group biting a pencil to

simulate the facial muscles of a smile. It was found that the group that had to bite on a pencil rated the cartoon as being much more amusing and likeable than the group that did not. Fuente: Tipton H. y Krause M. (2005).

[xxi] Traducido de *3. Cognition.* The cognitive component is the thoughtful, thinking aspect of our attitudes. Opinions toward an object or subject can be developed based solely on insightful, process-based thinking. It is no wonder that the nature of TV commercials during news programs is radically different than that aired on Saturday mornings. During news programs, people are more likely to be processing

information and "thinking." Fuente: Tipton H. y Krause M. (2005).

[xxii] El conjunto de componentes de hardware, conectados físicamente mediante cables u ondas, y configurados de una manera homogénea y sincronizada, que permiten establecer comunicaciones entre sí. (Katz, 2013)

UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE CIENCIAS ECONÓMICAS

DOCTORADO

TESIS

PROPUESTA DE UN MODELO CONTABLE QUE REFLEJE EL CARÁCTER DE ACTIVO QUE LA INFORMACIÓN CORPORATIVA REPRESENTA PARA UNA ENTIDAD BANCARIA

Alumno: Diego Sebastián Escobar

Directora de Tesis: Elsa Beatriz Suarez Kimura