

Definición de activos de información. Hacia un inventario de integral.

Diego Sebastián Escobar.

Cita:

Diego Sebastián Escobar (2025). *Definición de activos de información. Hacia un inventario de integral. XXXVII Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. Colegio de Graduados en Ciencias Económicas de CABA, Buenos Aires.*

Dirección estable: <https://www.aacademica.org/escobards/87>

ARK: <https://n2t.net/ark:/13683/ptuD/YNo>



Esta obra está bajo una licencia de Creative Commons.
Para ver una copia de esta licencia, visite
<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.es>.

Acta Académica es un proyecto académico sin fines de lucro enmarcado en la iniciativa de acceso abierto. Acta Académica fue creado para facilitar a investigadores de todo el mundo el compartir su producción académica. Para crear un perfil gratuitamente o acceder a otros trabajos visite: <https://www.aacademica.org>.

XXXVII Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos

***Título: “Definición de activos de información. Hacia un
inventario de integral.”***

Área: Contabilidad y Auditoría

Octubre de 2025

*Autor: **Diego Sebastián Escobar***

Maipú 429, Piso 5 Depto. 3, CP 1006, CABA.

Tabla de contenido

1. Introducción.....	4
2. Conceptualización de activo contable	4
3. Definición de activo de información	6
4. Categorías de activo de información	6
Información en custodia de la organización	6
Información en custodia de terceras partes:	7
Vinculación de los activos de información.....	8
5. Hacia un inventario de activos de información	9
6. El sistema de activos de información contable.....	10
7. Estándares internacionales en el manejo de activos de información.....	13
8. Información brindada por el SAIC	14
9. Reflexiones finales	15
Bibliografía.....	18

Definición de activos de información. Hacia un inventario de integral.

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 artículo se plantea identificar una definición de activo de información que cumpla con las características para un Modelo Contable no monetario para entidades bancarias.

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.

Como se indicó precedentemente, en el Marco conceptual del IASB se ha definido como activo a: “*un recurso económico presente controlado por la entidad como resultado de sucesos pasados.*”¹ (El Marco Conceptual para la Información Financiera, 2020). En esta

¹ En el Marco conceptual del IASB se ha definido como activo a: “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” **Fuente especificada no válida.**

línea, la Federación Argentina de Consejos Profesionales de Ciencias Económicas (FACPCE) en la Resolución Técnica N°16 ha establecido que:

“Un ente tiene un activo cuando, debido a un hecho ya ocurrido, controla los beneficios económicos que produce un bien (material o inmaterial con valor de cambio o de uso para el ente).

Un bien tiene valor de cambio cuando existe la posibilidad de:

- a) canjearlo por efectivo o por otro activo;*
- b) utilizarlo para cancelar una obligación; o*
- c) distribuirlo a los propietarios del ente.*

Un bien tiene valor de uso cuando el ente puede emplearlo en alguna actividad productora de ingresos.

En cualquier caso, se considera que un bien tiene valor para un ente cuando representa efectivo o equivalentes de efectivo o tiene aptitud para generar (por si o en combinación con otros bienes) un flujo positivo de efectivo o equivalentes de efectivo.

De no cumplirse este requisito, no existe un activo para el ente en cuestión.”

(RT N° 16: Marco Conceptual de las Normas Contables Profesionales, 2008)

Tomando como base las definiciones precedentes, la información y los datos procesados en las entidades bancarias, se encuentran bajo su custodia y consecuentemente controlan los beneficios económicos que este bien produce.

Por lo tanto, puede deducirse que la información forma parte del rubro del activo en los términos contables en el segmento patrimonial o financiero, pudiendo tener un valor de cambio y un valor de uso. En esta línea, 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, solamente 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 investigación.

3. Definición de activo de información

Como se indicó precedentemente, la información existente en las entidades bancarias se encuentra bajo su custodia, e independiente de su origen² se encuentra controlada por ellos mismos, y en consecuencia a los beneficios económicos que este bien inmaterial produce.

Dentro de las buenas prácticas, se destaca la serie IRAM/ISO/IEC 27.000 que define activo de información 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 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.

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:

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.

² Dado que la titularidad legal de ciertos datos existentes en las compañías corresponde a sus clientes, la entidad tiene la custodia de esta.

- **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 existente³. 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.

Información en custodia de terceras partes:

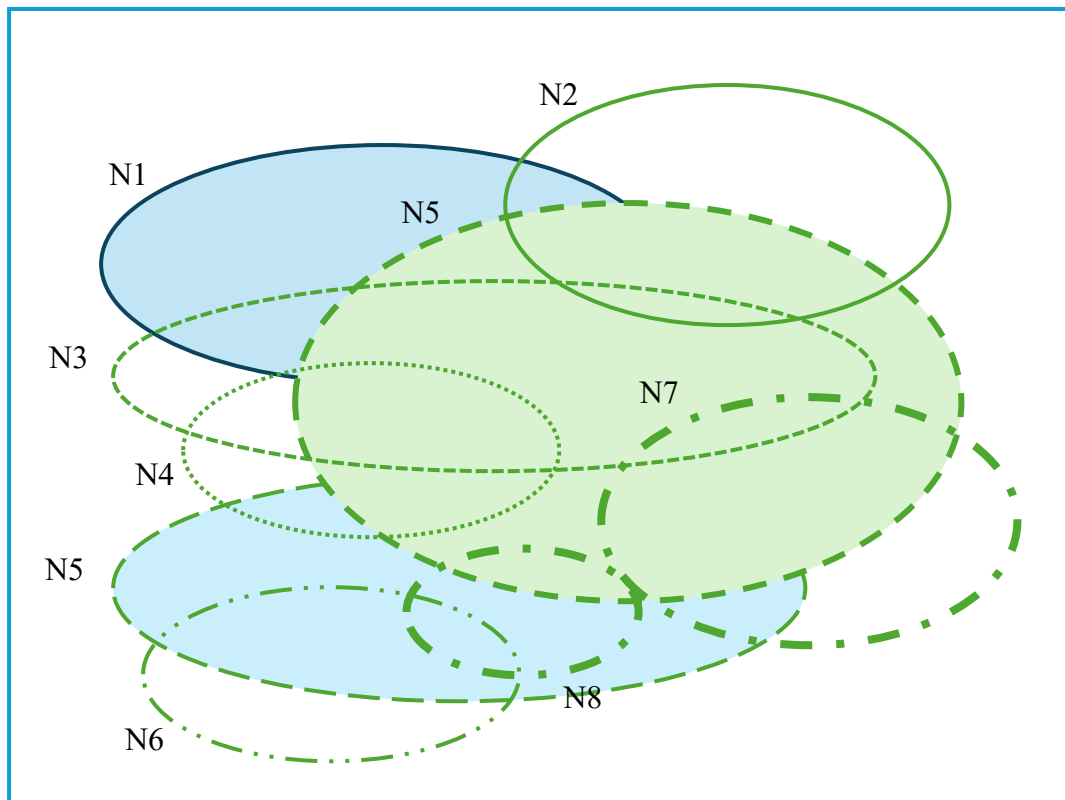
Al identificar la información es custodia de terceras partes, se pueden destacar:

- **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:

³ 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.

ESQUEMA N°1: Subconjuntos de activos de información



Fuente: Elaboración propia.

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 necesarios 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 tomada en cuenta cuando se definan las características del sistema de activos de información.

5. Hacia un inventario de activos de información

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 artículo 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.
- Recoleccionar 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).

6. 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 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*”, 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°2: Elementos básicos del sistema de activos de información contable elementos (SAIC).



Fuente: Elaboración propia.

7. 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°3: 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)

8. 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 de 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, 2013)

A los interesados en identificar las métricas básicas que deberían considerarse en el tablero de comando del SAIC, en el Anexo N°1 de la presente investigación se desarrollarán los indicadores a nivel estratégico, táctico y operativo a implementar en las entidades bancarias.

9. Reflexiones finales

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 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

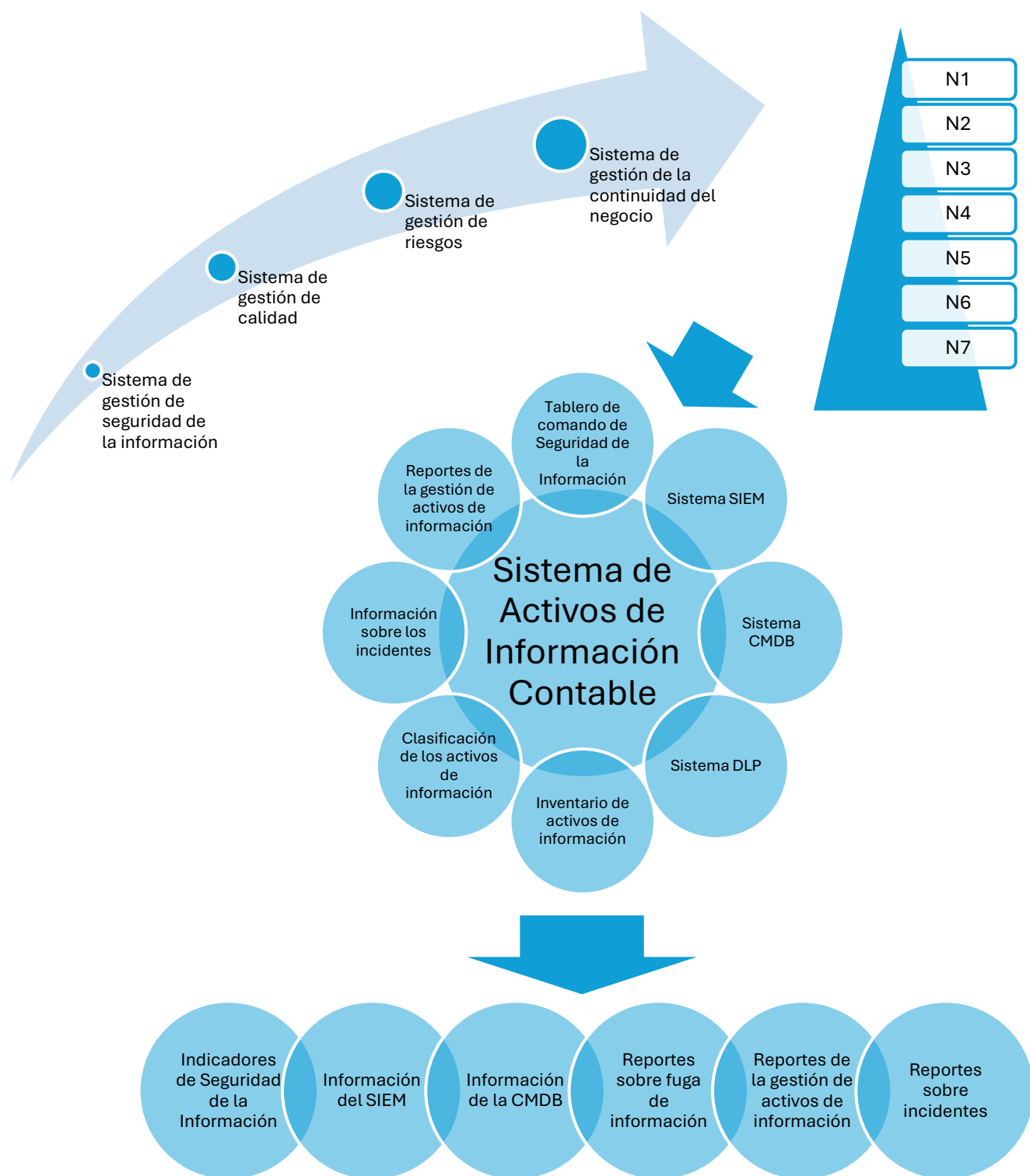
- Reportes de seguridad que registren la asignación de claves y derechos de accesos empleo de programas de utilidad que permitan el manejo de datos por fuera de las aplicaciones
- Reportes de seguridad de actividades de los usuarios privilegiados
- Reportes de seguridad de usuarios de emergencia y con 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 (CMDDB)
- 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°4: Relaciones del SAIC y los sistemas de gestión



Fuente: Elaboración propia.

Bibliografía

- 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>
- Comisión Nacional de Valores. (22 de enero de 2020). *CNV*. Obtenido de Sitio de la CNV: <http://www.cnv.gov.ar/leyesyreg/cnv/esp/rgcrgn629-14.htm>
- 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. (2025). Identificación de elementos para la elaboración de un marco conceptual no monetario de activos de información. *Contabilidad y Auditoría*, (61), 77-116.
- Escobar, D. S. (2024). Evaluación de las prácticas de ciberseguridad en micro y pequeños estudios contables del AMBA. In *JORNADA DE INVESTIGACIÓN. UNIVERSIDAD DEL SALVADOR FACULTAD CIENCIAS ECONÓMICAS Y EMPRESARIALES-USAL*.
- Escobar, D. S. (2024). Modelo capacitación y sensibilización en ciberseguridad para Contadores Públicos. In *JORNADA DE INVESTIGACIÓN 2024. FACULTAD CIENCIAS ECONÓMICAS Y EMPRESARIALES-USAL*.
- Escobar, D. S. (2023). CIBERRESILIENCIA: UN NUEVO DESAFÍO EN LA FORMACIÓN DEL CONTADOR PÚBLICO. In *XLIV Simposio Nacional de Profesores de Práctica Profesional. Universidad Nacional de Córdoba*.
- Escobar, D. S. (2023). Asegurando la Resiliencia Empresarial: Conceptos fundamentales a considerar en la auditoría de la continuidad del negocio. In *XXXV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. CGCE*.
- Escobar, D. S. (2023). Análisis de los cambios en los controles tecnológicos de la Comunicación A 7724 del BCRA en las entidades financieras. In *XXXV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. CGCE*.
- Escobar, D. S. (2023). EL IMPACTO DE LAS NUEVAS TECNOLOGÍAS DE INFORMACIÓN EN LA FORMACIÓN PROFESIONAL DEL CONTADOR. In *XLIV Simposio Nacional de Profesores de Práctica Profesional. Universidad Nacional de Córdoba*.
- Escobar, D. S. (2023). La profesión contable ante los desafíos de la inteligencia artificial Chat GPT. In *XXVI Congreso Nacional de Contabilidad. Colegio de Contadores del Paraguay*.
- Escobar, D. S. (2022). Requisitos mínimos de concientización para usuarios de Canales Electrónicos. *Publicaciones de la Comisión de Estudios sobre Sistemas de Registro*, (2-3), 1-8.
- Escobar, D. S. (2022). Identificación de estándares de seguridad de la información aplicables a los sistemas de información contable digitalizados. In *XLIII Simposio Nacional de Profesores de Práctica Profesional. UNCUIYO*.
- Escobar, D. S. (2022). Propuesta de un modelo contable que refleje el carácter de activo que la información corporativa representa para una entidad bancaria (Doctoral dissertation, Universidad de Buenos Aires (UBA)).
- Escobar, D. S. (2022). El rol del Contador en la era digital. In *VI Jornadas de Orientación Vocacional. UBA*.
- Escobar, D. S. (2022). Universo o dominio del discurso contable de los activos de información. In *ECON 2022. UBA*.
- Escobar, D. S. (2022). Identificación de los riesgos de los registros contables alojados en servicios de computación en la nube. In *XLIII Simposio Nacional de Profesores de Práctica Profesional. UNCUIYO*.
- Kimura, E. B. S., & Escobar, D. S. (2021). Gestión de la ciberseguridad en sistemas contables digitalizados. In *Ciclo" Universidades Iberoamericanas Dialogan". UBA*.
- Escobar, D. S. (2021). Mejores políticas para reducir los riesgos de alojar el sistema de información en la Nube. In *ECON 2021. Facultad de Ciencias Económicas*.
- Escobar, D. S. (2018). Replanteo en el análisis de las contingencias, oportunidades y amenazas de los desvíos en los Estados Financieros Prospectivos. *Gestión Joven*, (18), 11.

- 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 continua.
- Congreso de la República Argentina. (19 de abril de 2022). Ley N°25.326. Obtenido de Infoleg: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>
- 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.
- Federación Argentina de Consejos Profesionales de Ciencias Económicas. (2008). *RT N° 16: Marco Conceptual de las Normas Contables Profesionales*. Buenos Aires: FACPCE.
- 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.
- López, P., Moya, F., Marimón, S., & Planas, I. (2011). *Protección de datos de salud. Criterios y plan de seguridad*. Madrid: Diaz de Santos.
- Peso Navarro, E. d., Ramos, M. A., & Peso, M. d. (2004). *El documento de Seguridad (Análisis Técnico y Jurídico. Modelo)*. Madrid: Diaz de Santos.
- Portantier, F. (2013). *Gestión de la Seguridad Informática*. Buenos Aires: Fox Andina en coedición con DÁLAGA SA.
- 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.