

El Sistema de Activos de Información Contable (SAIC): Propuesta de identificación y definición conceptual.

Diego Sebastián Escobar.

Cita:

Diego Sebastián Escobar (2025). *El Sistema de Activos de Información Contable (SAIC): Propuesta de identificación y definición conceptual. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, 6 (1), 1-14.*

Dirección estable: <https://www.aacademica.org/escobards/90>

ARK: <https://n2t.net/ark:/13683/ptuD/e7H>



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>.

Ciberseguridad

El Sistema de Activos de Información Contable (SAIC): Propuesta de identificación y definición conceptual

Diego Sebastián Escobar

ORCID: <https://orcid.org/0009-0003-6913-5536>

Profesor Adjunto de Tecnología de la Información. Facultad de Ciencias Económicas y Empresariales de la Universidad del Salvador.

1. Introducción

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).

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*”¹, se deben implementar adecuadamente:

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

¹ En el punto 3.1.4.1. de la Comunicación “A” 4609 del BCRA.

- Registros de las funciones utilizadas
- Reportes de seguridad que registren la asignación de claves y derechos de acceso 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.

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°1: Elementos básicos del sistema de activos de información contable elementos (SAIC).



Fuente: Elaboración propia.

3. El inventario de activos de información en entidades bancarias

El BCRA 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.”

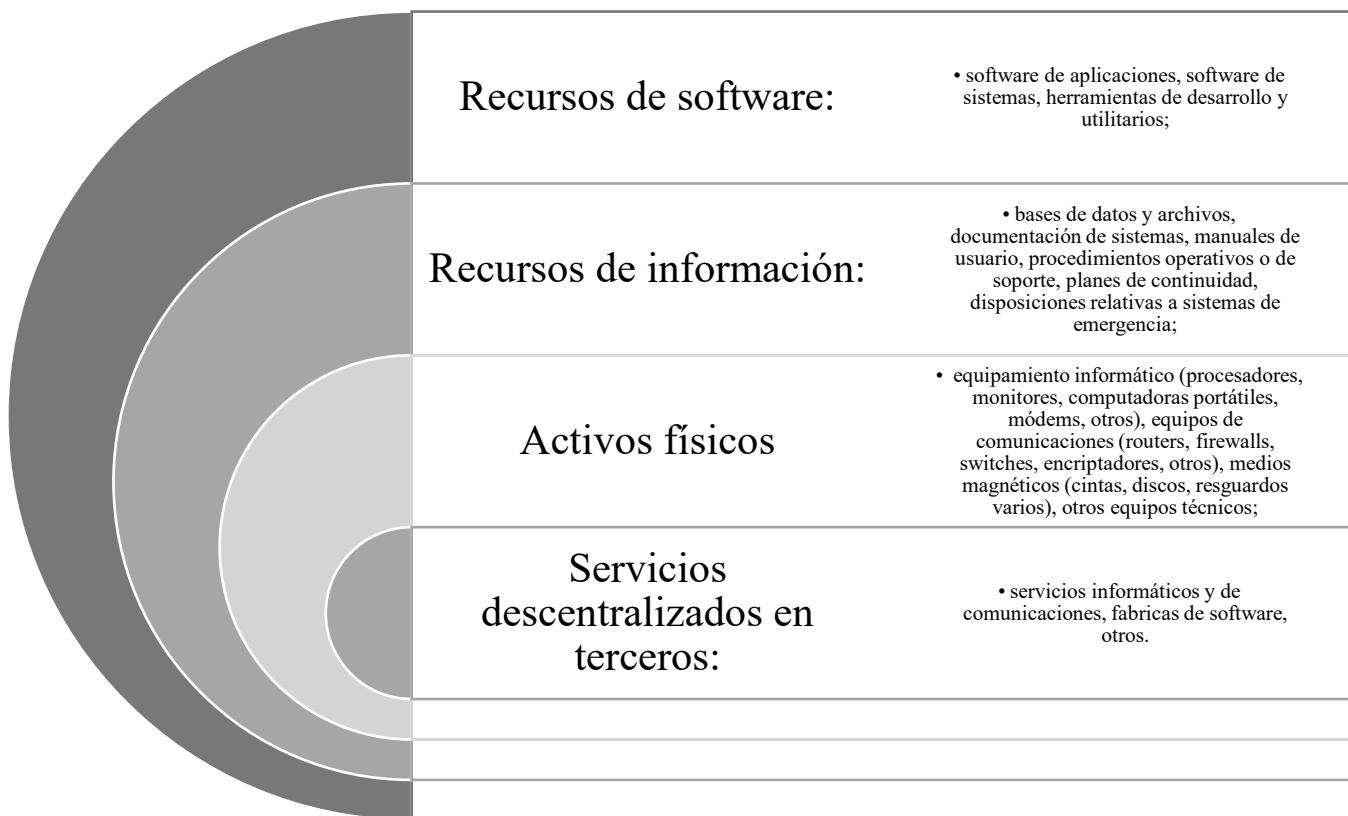
En este caso, el organismo de control instruye que las entidades deben establecer un inventario de activos de información, considerando las categorías indicadas en el capítulo anterior. Asimismo, indica que deben contar con procedimientos para identificar sus activos que pueden ser por procesos manuales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

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.”

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°2: 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°3: Requerimientos al Sistema Contable de Activos de Información.

Requerimientos del BCRA al sistema contable de activos de información	Consideraciones
<p><i>“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.”</i></p>	<p>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.</p>
<p><i>“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 información, o formar un documento aparte.”</i></p>	<p>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). Se debe documentar todos los procedimientos de esta sistematización.</p>

<p><i>“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.”</i></p>	<p>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.</p>
<p>Fuente: (BCRA, 2006)</p>	

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).

4. 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.

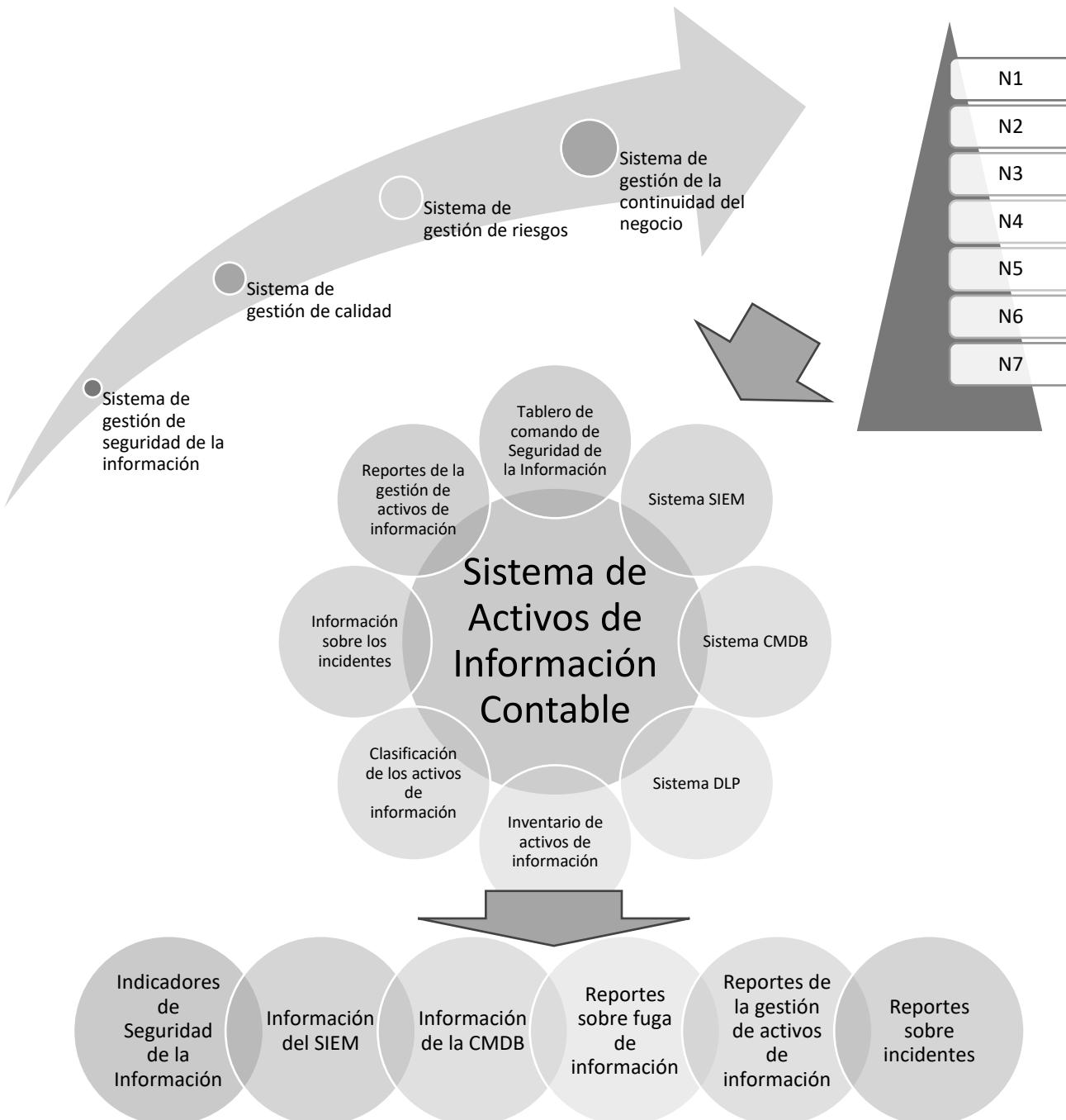
Bajo estos requisitos, el sistema de activos de información contable (SAIC) en las entidades bancarias está compuesto mínimamente por los siguientes componentes:

- 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°4: Relaciones del SAIC y los sistemas de gestión



Fuente: Elaboración propia.

5. Bibliografía

- 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.
- 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/rccrgn629-14.htm>
- Escobar, D. S. (2010). Ley de Protección de Datos Personales. Revista Imagen Profesional, de La Federación Argentina de Consejos Profesionales en Ciencias Económicas.
- 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., & Vera, A. (2024). Análisis de las variables de ciberseguridad en micro y pequeños estudios contables del AMBA. In Tercera Jornada Institucional de Investigación de la Universidad del Salvador. USAL.
- 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. (2025). Ciberresiliencia Inteligente: Aplicaciones de la IA en la Seguridad Digital. In Conferencia Online-Comisión Técnica• Sistemas y TI. AIC-Comisión Técnica• Sistemas y TI.
- Escobar, D. S. (2024). Aplicaciones, desafíos y ciberresiliencia de la inteligencia artificial y el chat GPT en la profesión contable. In Conferencia Online-Comisión Técnica• Sistemas y TI. AIC-Asociación Interamericana de Contabilidad.
- Escobar, D. S. (2024). Segmentos y modelos contables aplicados a la información. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, 1(1), 1-13.
- Escobar, D. S. (2024). Desafíos y Competencias en la Formación del Contador: Exigencias del Siglo XXI. In XXXVI Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. Colegio de Graduados en Ciencias Económicas de la Ciudad Autónoma de Buenos Aires.
- Escobar, D. S. (2024). El Impacto de la IA en el Ámbito Contable: Desafíos y Oportunidades para los Contadores Públicos. In XXXVI Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. Colegio de Graduados en Ciencias Económicas de la Ciudad Autónoma de Buenos Aires.
- Escobar, D. S. (2024). Definición teórica de Activo de información. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, 1(2), 1-13.
- 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. CIBERRESILIENCIA: UN NUEVO DESAFÍO EN LA FORMACIÓN DEL CONTADOR (Doctoral dissertation, Universidad de Buenos Aires).
- Escobar, D. S. (2023). Características a considerar en la elaboración de planes de concientización en Ciberseguridad para Contadores Públicos. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, (3-1), 1-7.
- Escobar, D. S. (2021). Actualización en los estándares de seguridad de la información aplicables a los sistemas de información contable digitalizados. In SIMPOSIO NACIONAL DE PROFESORES DE PRÁCTICA PROFESIONAL.
- 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). Implementación del inventario de activos de información en entidades financieras: Desafíos y estándares aplicables. In XXXIV Jornadas Profesionales de Septiembre de 2025

- Contabilidad, Auditoría y de Gestión y Costos. Colegio de Graduados en Ciencias Económicas.
- Kauf, A., & Escobar, D. S. Implementación profesional de un proyecto de desarrollo de métricas de seguridad informática para entidades financieras.
- 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 Organizaciones 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.