Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, vol. 6, núm. 4, 2025, pp. 1-17.

Propuesta de Indicadores de Seguridad para la Gestión de Activos de Información.

Diego Sebastián Escobar.

Ciberseguridad

Propuesta de Indicadores de Seguridad para la Gestión de Activos de Información

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.

Diciembre de 2025

- Contenido

1. Introducción 2

2. Indicadores estratégicos 3

3. Indicadores tácticos y operativos estratégicos 9

4. Reflexiones finales 15

5. Bibliografía 16

1. Introducción

El presente artículo tiene como objetivo principal proponer un conjunto de indicadores de seguridad aplicables al control y gestión de los activos de información en entes. Los indicadores desarrollados se agrupan en dos categorías: estratégicos y táctico-operativos, con el fin de brindar una visión integral tanto para la alta dirección como para los equipos técnicos.

Para su elaboración se consideraron marcos y estándares ampliamente reconocidos, entre ellos COBIT 5, COSO II, IRAM/ISO/IEC 27002, así como las recomendaciones de seguridad propuestas por Mauricio Ramírez (2017).

Este enfoque multidimensional permite asegurar que los indicadores propuestos se alineen con buenas prácticas internacionales y resulten aplicables al contexto argentino.

2. Indicadores estratégicos

A continuación, se exponen los indicadores estratégicos más relevantes para la protección de los activos de información en entes:

ESQUEMA N°1: Indicadores estratégicos sobre seguridad y privacidad de la información

Objetivo	Característica de la métrica	Periodicidad
Documentar todos los procesos de la organización.	Identificar el porcentaje de procesos documentados en la entidad.	Semestral
Definir, desarrollar, implementar y actualizar políticas, normas, procedimientos, estándares, formularios e instructivos que conformen todos los procesos de la entidad.	Identificar el porcentaje de actualización de políticas.	Anual
	Identificar el porcentaje de actualización de normas.	Anual
	Identificar el porcentaje de actualización de procedimientos.	Anual
Documentar y verificar la implementación del modelo de documentación de procesos establecidos y de los futuros a implementar.	Identificar el porcentaje de procesos operativos que están implementados.	Trimestral
Verificar el 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°2: Indicadores estratégicos sobre capacitación y concientización de los recursos humanos

Objetivo	Característica de la métrica	Periodicidad
Analizar 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
Verificar la continuidad del plan de concientización y capacitación.	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°3: Indicadores estratégicos sobre los riesgos de los activos de información

Objetivo	Característica de la métrica	Periodicidad
Involucrar a 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 contestaron	Trimestral

	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
Identificar, evaluar, analizar, tratar y documentar los riesgos de los activos de información formal y periódicamente.	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
Tratar eficazmente 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

Mejorar la efectividad 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°4: Indicadores estratégicos sobre el cumplimiento normativo

Objetivo	Característica de la métrica	Periodicidad
Solucionar las observaciones de auditoría 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°5: Indicadores estratégicos sobre información de gestión

Objetivo	Característica de la métrica	Periodicidad
Reportar en forma periódica 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°6: Indicadores estratégicos sobre la arquitectura de seguridad

Objetivo	Característica de la métrica	Periodicidad
Participar 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
Optimizar 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
Documentar los estándares de seguridad para las distintas plataformas.	Calcular el porcentaje de estándares de “hardening” definidos en relación con las plataformas utilizadas.	Semestral
Analizar la recurrencia de incidentes	Indicar la cantidad de incidentes recurrentes en los activos de información.	Mensual
Minimizar 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
Solucionar las vulnerabilidades identificadas	Indicar la cantidad de vulnerabilidades pendientes de corrección.	Mensual

ESQUEMA N°7: Indicadores estratégicos sobre los canales electrónicos

Objetivo	Característica de la métrica	Periodicidad
Monitorear y controlar todos los canales electrónicos de la entidad	Calcular el porcentaje de canales críticos que tienen activado el registro de eventos de seguridad.	Mensual
Analizar el 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
Asegurar la designación de un responsable de negocio por cada canal electrónico	Indicar la cantidad de canales que no tienen propietario definido.	Mensual

ESQUEMA N°8: Indicadores estratégicos sobre monitoreo y control

Objetivo	Característica de la métrica	Periodicidad
Evaluar el proceso de monitoreo.	Calcular el porcentaje de vulnerabilidades e incidentes detectados.	Mensual
	Calcular el porcentaje de controles implementados respecto al total planificado.	Mensual
Detectar eventos de seguridad que no están registrados en el Sistema de Activos de Información Contable.	Indicar la cantidad de eventos críticos detectados no contemplados en el Sistema de Activos de Información Contable.	Mensual
Asegurar la correcta segregación de puestos funcionales	Calcular el porcentaje de usuarios críticos cuyos accesos son consistentes con el puesto funcional asignado.	Mensual

Verificar privilegios otorgados a los usuarios	Calcular el porcentaje de sistemas, servicios y/o aplicaciones críticas, para las cuales se realiza un control periódico de niveles y privilegios otorgados.	Mensual

3. Indicadores tácticos y operativos estratégicos

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

ESQUEMA N°9: Indicadores tácticos y operativos de riesgo de activos de información

Objetivo	Característica de la métrica	Periodicidad
Documentar 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
Anticipar la ocurrencia de incidentes, a través de una gestión de riesgos eficaz.	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

Corregir las debilidades que expongan a la entidad a niveles inaceptables.	Calcular el grado de cumplimiento general normalizado con respecto a la Comunicación “A” 4609 del BCRA.	Trimestral

ESQUEMA N°10: Indicadores tácticos y operativos de gestión de incidentes

Objetivo	Característica de la métrica	Periodicidad
Verificar la comunicación de incidentes y vulnerabilidades.	Calcular el porcentaje de incidentes y vulnerabilidades comunicados dentro de un margen de tiempo establecido.	Mensual
Verificar que los incidentes y vulnerabilidades sean notificados a la autoridad competente.	Calcular el porcentaje de incidentes y vulnerabilidades notificados a la gerencia o propietario de información.	Mensual
Verificar los incidentes conocidos y no reportados	Calcular el porcentaje de incidentes y vulnerabilidades conocidos y no reportados	Mensual
Evaluar el proceso de monitoreo.	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

Detectar la asignación de operaciones incompatibles con la segregación de puestos funcionales.	Indicar la cantidad de casos detectados relacionados con la asignación de roles contrapuestos.	Mensual
Verificar periódicamente los niveles y privilegios otorgados a los usuarios	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°11: Indicadores tácticos y operativos de administración de accesos

Objetivo	Característica de la métrica	Periodicidad
Asegurar que los derechos de acceso se otorguen a través de un proceso de autorización formal del propietario de los datos	Indicar la cantidad de accesos no autorizados detectados en un período de tiempo	Diaria
Implementar métodos de identificación y autenticación para controlar el acceso a los sistemas y servicios informáticos, en el marco de políticas de usuario y contraseña.	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 alineadas con el estándar del BCRA.	Diaria
	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
Automatizar el otorgamiento y revocación de accesos y errores de operador	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
Registrar y controlar periódicamente la asignación y utilización de usuarios especiales.	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
Restringir la posibilidad de accesos concurrentes.	Calcular el porcentaje de sistemas, servicios o aplicaciones críticos para los cuales el acceso concurrente se encuentra restringido.	Mensual

ESQUEMA N°12: Indicadores tácticos y operativos de fuga de información

Objetivo	Característica de la métrica	Periodicidad
Aplicar 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
Restringir la gestión de información sensible al ámbito de repositorios seguros.	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°13: Indicadores tácticos y operativos de incidentes

Objetivo	Característica de la métrica	Periodicidad
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 instalaciones que contienen sistemas de información.	Mensual
	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
Implementar 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 seguridad pendientes de implementación.	Mensual
	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 conteniendo software no autorizado.	Mensual
	Indicar la cantidad de incidentes causados por la instalación de software no autorizado.	Mensual

4. Reflexiones finales

El análisis desarrollado evidencia la necesidad de contar con un sistema integral de indicadores que permita evaluar, de manera sistemática y continua, la seguridad de los activos de información en el ámbito bancario. La propuesta presentada —estructurada en indicadores estratégicos y táctico-operativos— se sustenta en marcos conceptuales ampliamente reconocidos, tales como COBIT 5, COSO II e IRAM/ISO/IEC 27002.

Los indicadores estratégicos permiten comprender el grado de madurez institucional respecto de la documentación de procesos, la gestión del riesgo, la arquitectura de

seguridad, el cumplimiento normativo y la efectividad de las prácticas de capacitación y concientización del personal. Su enfoque macro posibilita evaluar la capacidad de gobierno, la consistencia de las políticas y la integración de la seguridad en la planificación organizacional, aspectos fundamentales en entidades donde la información constituye un activo crítico.

Complementariamente, los indicadores tácticos y operativos aportan una visión detallada de la ejecución cotidiana de los controles y procesos vinculados con la seguridad de la información. Su alcance incluye la administración de accesos, el tratamiento de vulnerabilidades, la detección y respuesta ante incidentes, la prevención de fuga de información y la operación de mecanismos técnicos de protección. Estas métricas permiten monitorear desviaciones, identificar oportunidades de mejora y sustentar decisiones basadas en evidencia.

En este sentido, el modelo propuesto constituye una herramienta valiosa para incrementar la resiliencia organizacional y asegurar la protección efectiva de los activos de información.

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/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.

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 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 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.