XLVI Simposio Nacional de Profesores de Práctica Profesional. UNIVERSIDAD SIGLO21, Córdoba, 2025.

Identificación de mejores prácticas y estándares de control aplicadas al control de los activos de información.

Diego Sebastián Escobar.

Cita:

Diego Sebastián Escobar (2025). *Identificación de mejores prácticas y estándares de control aplicadas al control de los activos de información. XLVI Simposio Nacional de Profesores de Práctica Profesional. UNIVERSIDAD SIGLO21, Córdoba.*

Dirección estable: https://www.aacademica.org/escobards/88

ARK: https://n2t.net/ark:/13683/ptuD/Quc

XLVI Simposio Nacional de Profesores de Práctica Profesional

UNIVERSIDAD SIGLO21

“Por la innovación, integración y la inspiración necesaria para acompañar el cambio en la Práctica Profesional”.

30 y 31 de octubre de 2025

Área: Actualización de contenidos programáticos.

Título: “Identificación de mejores prácticas y estándares de control aplicadas al control de los activos de información”

Autor: Dr. Diego Sebastián Escobar

Facultad de Ciencias Económicas - Universidad de Buenos Aires

Tabla de contenido

Resumen

En el marco del XLVI Simposio Nacional de Profesores de Práctica Profesional, se somete a análisis de todos los participantes el tratamiento de las normativas aplicables y estándares utilizados en la planificación, gestión y control de los activos de información. En el trabajo se destaca la importancia de abordar la seguridad de la información de manera interdisciplinaria, considerando tanto aspectos tecnológicos como organizacionales y humanos.

Normas y modelos principales

IRAM/ISO/IEC 27.001: Establece los requisitos fundamentales para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), abarcando la gestión, operación, supervisión y mejora continua del sistema.

COBIT: Proporciona lineamientos para el gobierno y control de TI, facilitando la creación de políticas y buenas prácticas para el control en todas las áreas de la organización.

NIST SP800-53 y SP800-30: Normas internacionales que influyen en el análisis de riesgos y controles de seguridad de los activos de información.

ITIL y Prince2: Modelos orientados a la gestión de servicios y proyectos de TI, con puntos de contacto relevantes para la seguridad.

ISM3 y SOGP: Enfoques novedosos que consideran la cultura organizacional y las buenas prácticas basadas en experiencias internacionales.

PCI DSS: Requisitos mínimos para la protección de datos de titulares de tarjetas, aplicables en el sector financiero.

COSO: Marco de referencia para el control interno, orientado al cumplimiento normativo, confiabilidad de la información financiera y eficiencia operativa.

Conclusión

El documento concluye que la gestión eficiente de los activos de información en organizaciones requiere la adopción de estándares internacionales, la implementación de buenas prácticas y la adaptación de los modelos de gestión a las necesidades específicas del negocio. La seguridad de la información debe ser vista como un proceso integral, que involucra tecnología, personas y organización.

Identificación de mejores prácticas y estándares de control aplicadas al control de los activos de información

1. Introducción

En el marco del XLVI Simposio Nacional de Profesores de Práctica Profesional, se somete a análisis de todos los participantes el tratamiento de las normativas aplicables y estándares utilizados en la planificación, gestión y control de los activos de información. Este enfoque resulta indispensable para comprender el dominio del discurso contable en modelos organizacionales contemporáneos, especialmente en el sector bancario, donde la información constituye un activo crítico.

El objetivo del presente artículo es analizar e identificar los marcos de gestión y buenas prácticas de Tecnología y Seguridad de la Información vigentes en las organizaciones, orientados a la administración de los activos de información bajo su custodia.

2. Interrelación de los activos de información

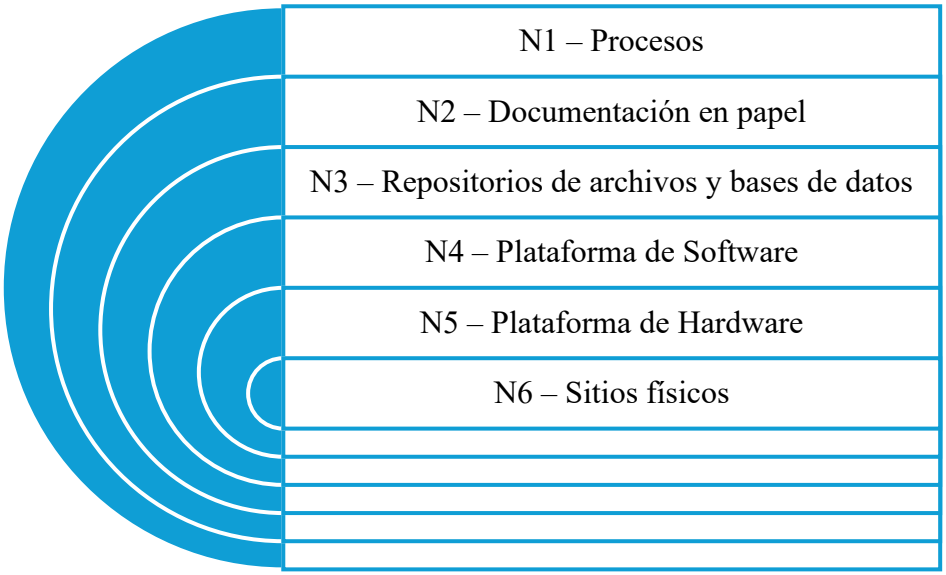
Los activos de información comprenden un conjunto diverso de elementos que conforman un universo complejo y dinámico. Por ello, resulta fundamental establecer las relaciones de dependencia y vinculación entre dichos componentes para garantizar una gestión eficaz y segura.

En una primera instancia, se identifican los procesos y procedimientos que estructuran el funcionamiento operativo de la entidad. Posteriormente, se procede a reconocer y asociar los distintos elementos que intervienen en dichos procesos, tales como la documentación física, los repositorios de datos, las aplicaciones, módulos y herramientas informáticas utilizadas, así como la infraestructura tecnológica y los sitios físicos donde se alojan o procesan los activos.

Finalmente, se consideran aquellos activos que, si bien no se encuentran bajo custodia directa de la entidad, son igualmente relevantes para su gestión, como los proveedores

externos y los recursos humanos vinculados a la operación, cuya interacción con los sistemas y procesos internos requiere controles específicos y políticas de seguridad adecuadas.

ESQUEMA N°1: 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 organizaciones:

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

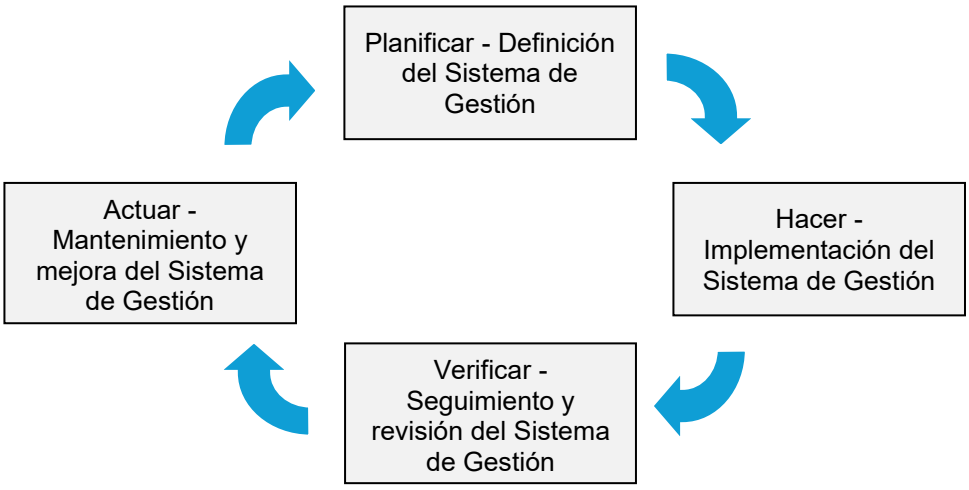
En esta sección se identificarán normas para analizar los procesos administrativos, de tecnología y de control interno.

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°2: 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°3: 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.

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°4: Informe COSO 2

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

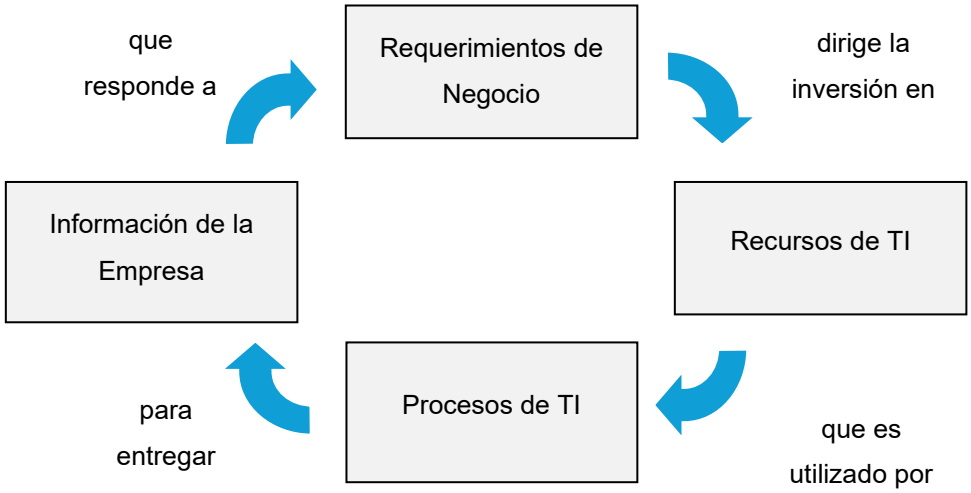
4. Estándares asociados a los activos de información N3 (Repositorios de archivos y bases de datos), N4 (Plataforma de Software) y N5 (Plataforma de Hardware).

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°5: Principios básicos de COBIT



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

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.

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.

5. Estándares asociados a todos los activos de información

5.1. IRAM/ISO/IEC 27.001

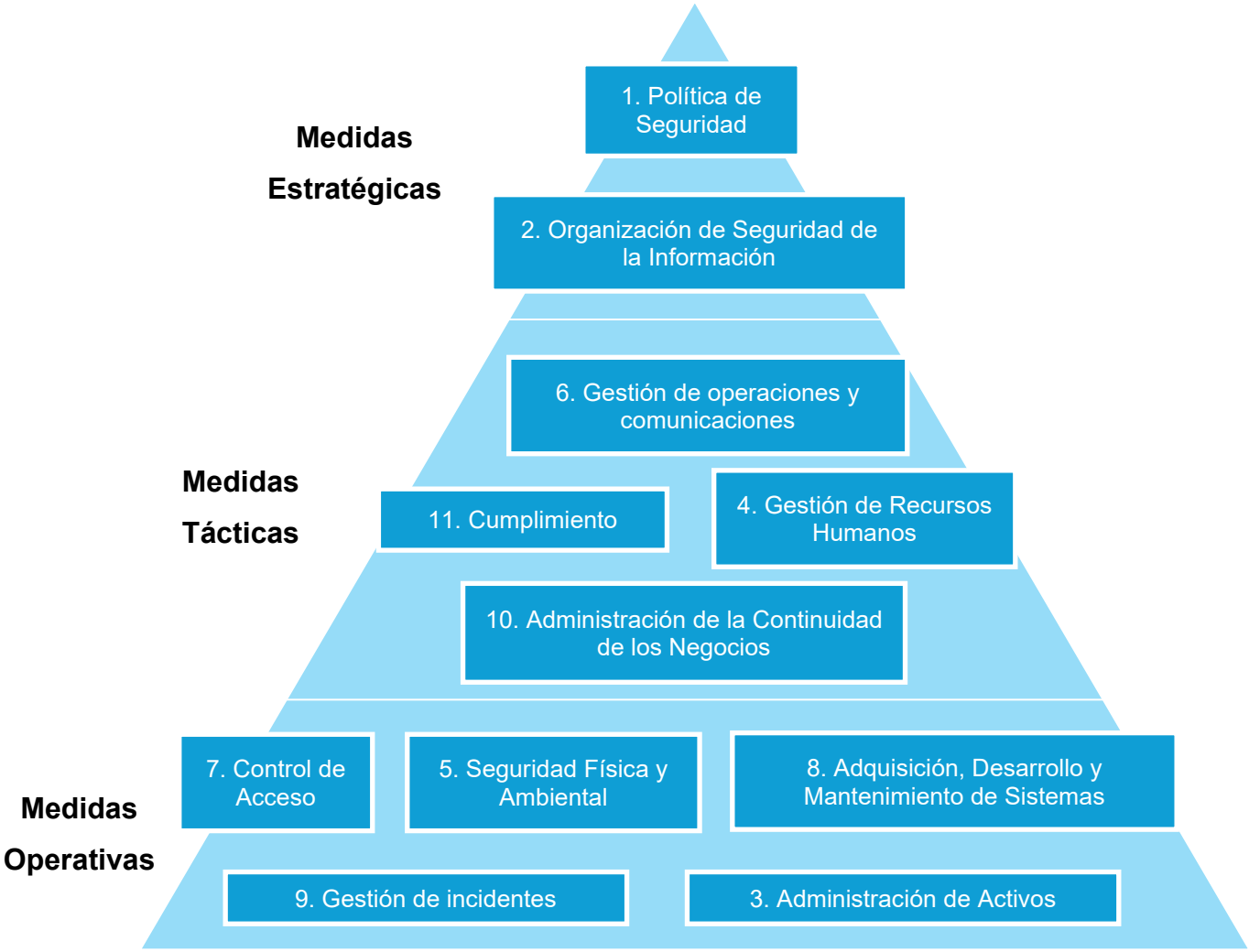
El Sistema de Gestión de Seguridad de la Información es definido como un "Proceso sistemático, documentado y conocido por toda la organización. Y basado en un enfoque por riesgo de negocio, el SGSI es un modelo para el establecimiento, implementación, operación, control, revisión, mantenimiento y mejora 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 dominios a tener en cuenta para implantar en la Gestión de la Seguridad.

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°6: Niveles organizacionales y los dominios establecidos por la IRAM/ISO/IEC 27.001

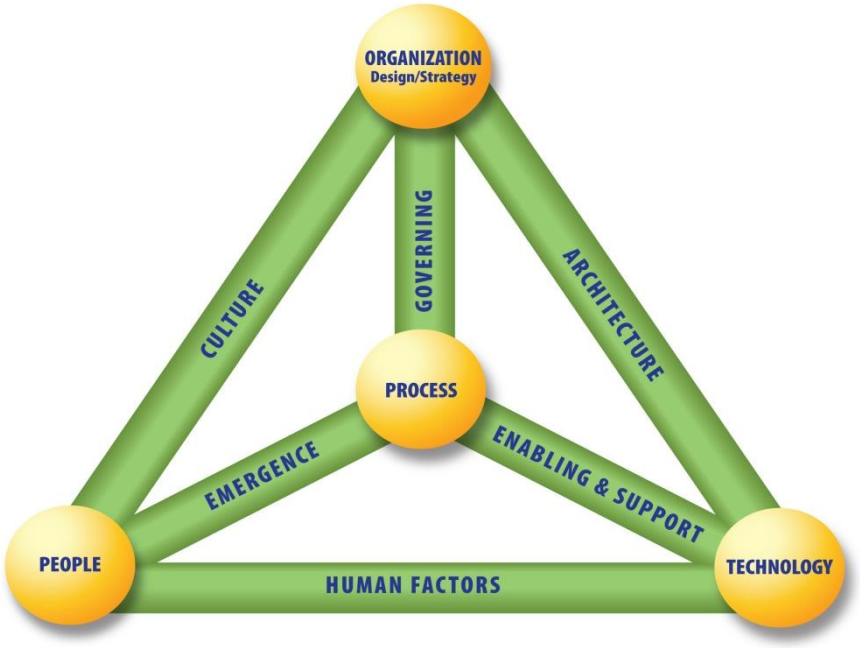


Fuente: (IRAM/ISO/IEC, 2018)

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°7: 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.

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.*"

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.

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, 2019).

6. Conclusiones

Las normas vigentes 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°8: 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°9: Análisis de los Modelos de Gestión de la Seguridad de la información y capacitación de los usuarios.

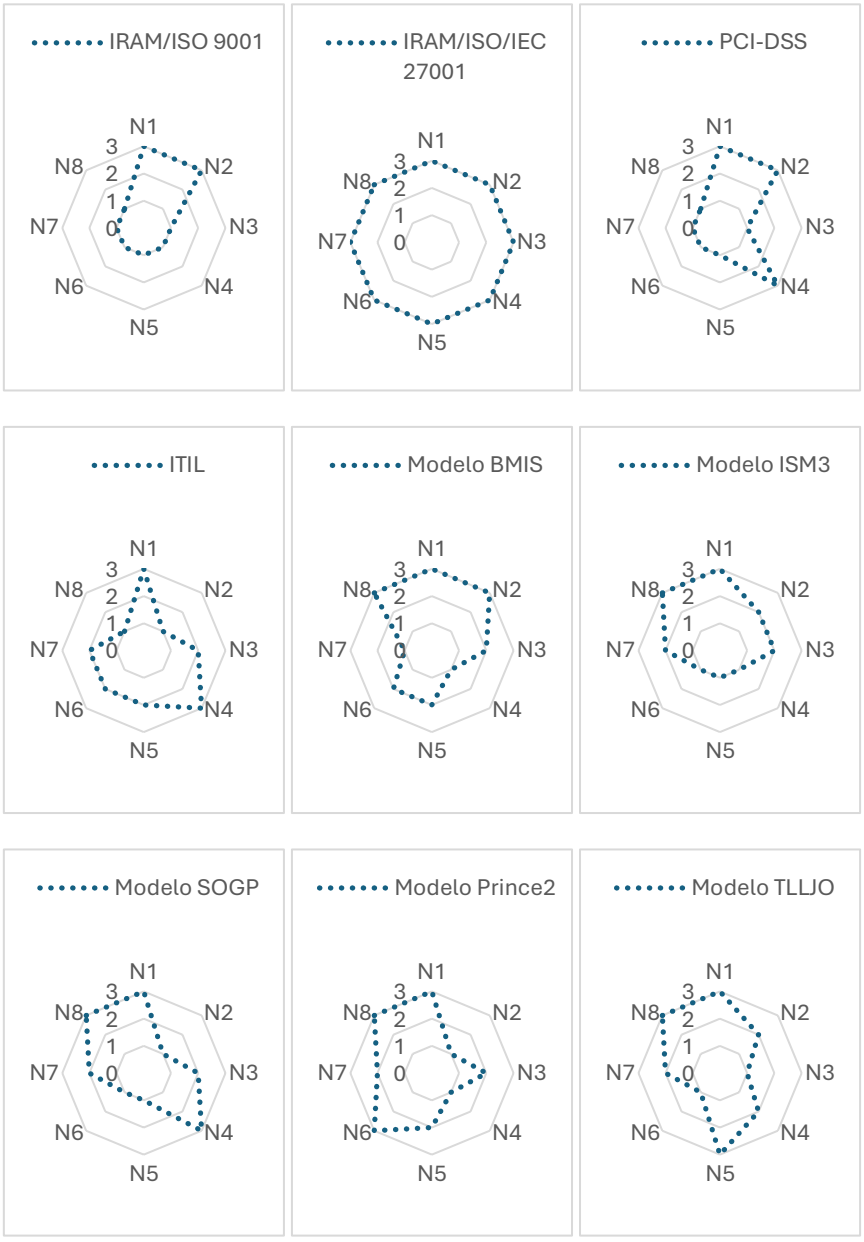
Modelos de Gestión de la Seguridad de la información			
Nombre	**Difusión**	**¿Adapta a las organizaciones?**	**Características**
Modelo de Negocio de Seguridad Informática o "The Business Model for Information Security"	Alta	SI	Toma como ejes fundamentales en la gestión de la seguridad a las personas,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

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.

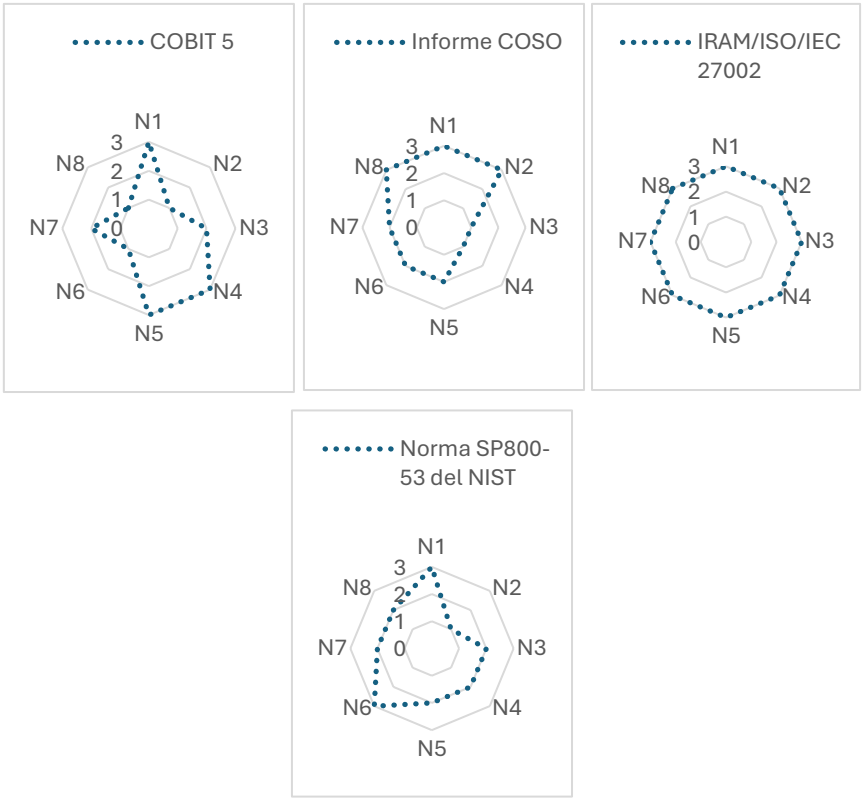
ESQUEMA N°10: Modelos de Gestión de la Seguridad de la Información



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°11: 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.

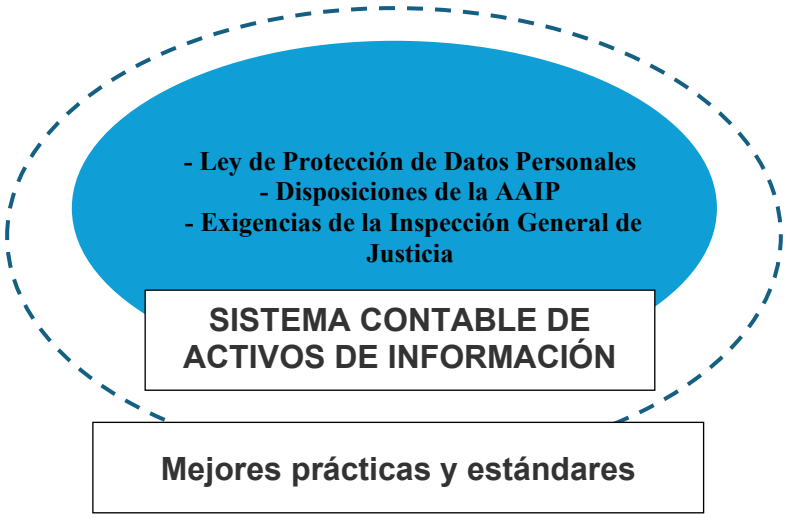
Para poder proteger a los activos en conocimiento de los empleados, proveedores y clientes de las organizaciones se plantea la necesidad de definir la gestión de la capacitación y concientización en Seguridad Informática.

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°12: 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.

7. Bibliografía

Committee of Sponsoring Organizations of the Tread. (2013). *Internal Control – Integraded Framework.* Edición digital.

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.

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. UNCUYO.

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. UNCUYO.

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.

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

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 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.

Portantier, F. (2019). *Seguridad Informática.* Buenos Aires: Fox Andina Dálaga.

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