XXXIV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos.
Colegio de Graduados en Ciencias Económicas, Buenos Aires, 2022.

Implementación del inventario de activos de información en entidades financieras: Desafíos y estándares aplicables.

Diego Sebastian Escobar.

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

Título: Implementación del inventario de activos de información en entidades financieras: Desafíos y estándares aplicables

Área: Contabilidad y Auditoría

1.9. Medidas preventivas para la seguridad informática dentro del marco de las organizaciones

Autor: ***Diego Sebastián Escobar***

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

Tabla de contenido

Implementación del inventario de activos de información en entidades financieras: Desafíos y estándares aplicables

1.1. Introducción

En el marco de las XXXIV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos organizadas por el Colegio de Graduados en Ciencias Económicas someto a la consideración de todos los participantes el análisis de la implementación del inventario de activos de información en las entidades financieras.

El objetivo del presente trabajo es identificar las características básicas que debe contener el inventario de activos de información y aquellos estándares o buenas prácticas aplicables.

1.2. Clasificación de los activos de información

El concepto de activo de información ha sido definido en la serie IRAM/ISO/IEC 27.000 como a *"los datos o conocimientos que tienen valor para una organización".* En las entidades financieras, se pueden identificar información en diversos tipos y principalmente se pueden destacar los que se encuentran en custodia de terceros o que se encuentran bajo el dominio del ente. A continuación se analizan ambas definiciones:

Información en custodia de la organización:

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

- **Procesos**.
- **Documentación en papel.**
- **Repositorios de archivos y bases de datos**.
- **Plataforma de Software.**
- **Plataforma de Hardware.**
- **Sitios físicos.**

Información en custodia de terceras partes:

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

- **Proveedores en servicios centralizados o tercerizados.**
- **Información en conocimiento del personal.**

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

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

1.3. Normativas identificadas en el Banco Central de la República Argentina

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

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

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

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

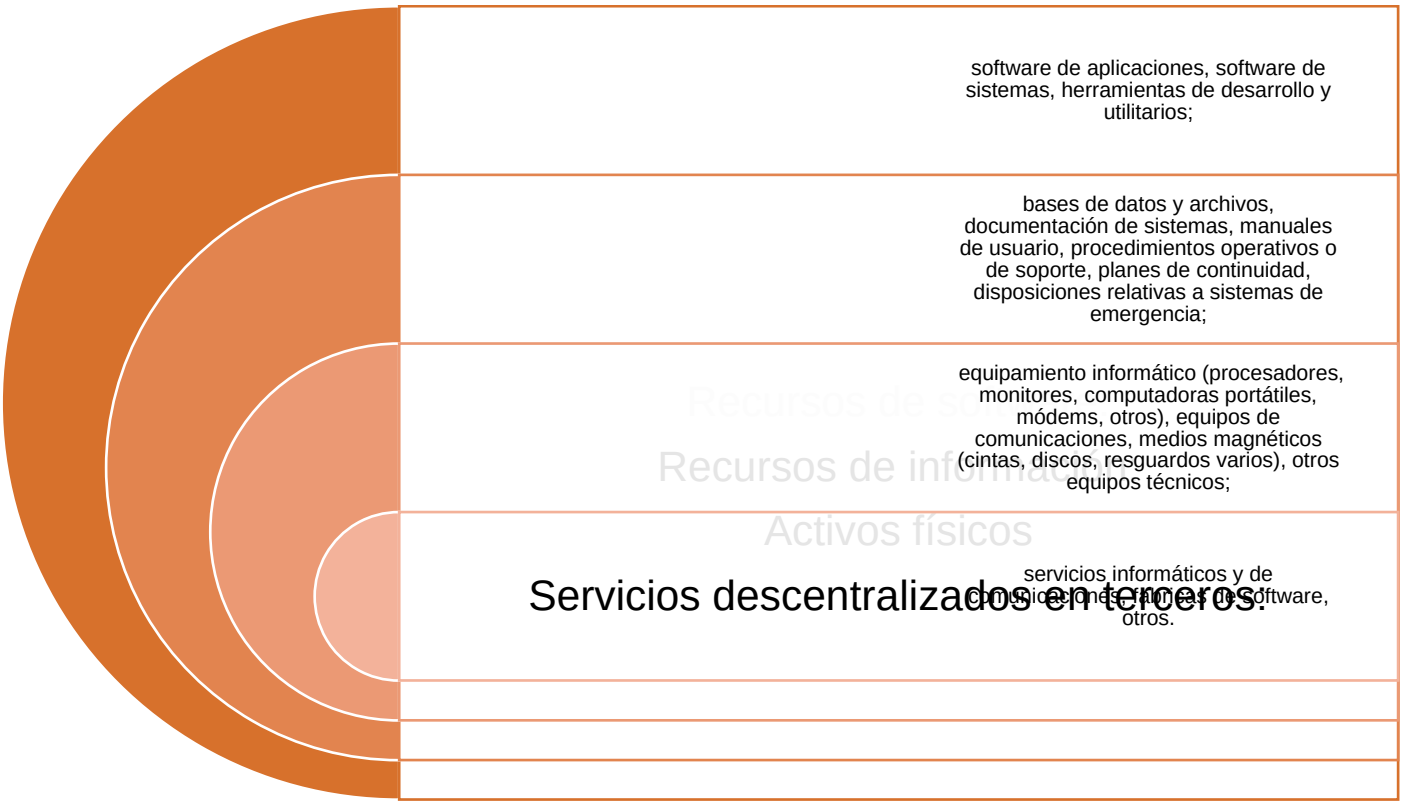
En este caso, el organismo plantea que las entidades asignen niveles de importancia, categorizándolos, clasificándolos y actualizándolos.

> *“Por ello, las entidades financieras deben elaborar y mantener un inventario de los activos asociados a cada sistema de información. Se debe identificar claramente cada activo, estableciendo su propietario y su clasificación en cuanto a seguridad.”* (BCRA, 2006).

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

Un óptimo inventario de activos de información debería contener el detalle de todos los componentes existentes y su relación. En esta línea el BCRA establece contener como mínimo los siguientes elementos:

ESQUEMA N°8: 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. En este sentido, se destaca que la información de gestión del inventario de los activos de información debe:

> "*permitir identificar el tipo de información que contienen, han de ser inventariados y además almacenados en lugares con acceso restringido sólo al personal autorizado. Los soportes que tengan datos protegidos, sea como consecuencia de operaciones temporales de la propia aplicación que los trata, o como consecuencia de procesos periódicos de apoyo o*

cualquier otra operación espontánea, deberán estar claramente identificados con una etiqueta externa que indique de qué datos se trata." (López, Moya, Marimón, & Planas, 2011)

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

1.4. Estándares internacionales en el manejo de activos de información

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:

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

ESQUEMA N°10: Controles del inventario de activos de información 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)

1.5. Reflexiones finales

Al considerar activo de información como *"los datos o conocimientos que tienen valor para una organización"* (IRAM/ISO/IEC 27.000) y teniendo en cuenta en quien recae la custodia de los datos, se pueden identificar dos clases de activos de información: los que se encuentran en custodia de la organización, identificados como: Procesos; Documentación en papel; Repositorios de archivos y bases de datos; Plataforma de Software; Plataforma de Hardware o Sitios físicos; y los que se encuentran en custodia de terceras partes, identificados como: Proveedores o información en conocimiento del personal.

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 la IRAM/ISO/IEC 27.002 se establecen controles para el inventario como: *"Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes*" y en relación con los propietarios 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*."

Por todo lo expuesto, el inventario de activos de información constituye un instrumento indispensable para el eficiente control en las organizaciones, si bien en el caso de las entidades financieras es de implementación obligatoria, es considerada como una buena práctica en el monitoreo y control de la información corporativa.

1.6. Bibliografía

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.

Suarez Kimura, E. B., & Escobar, D. S. (2010). Repercusiones de La Ley De Protección de Datos Personales en el Ejercicio Profesional del Contador Público. *Foro Nacional de Simposios de Profesores de Práctica Profesional*, Publicación contínua.

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.

AAIP. (19 de abril de 2022). *Agencia de Acceso a la Información Pública.* Obtenido de Disposición N° 11/2006: http://www.jus.gob.ar/datos-personales.aspx

BCRA. (04 de Enero de 2006). *Comunicación "A" 4609: "Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con*

tecnología informática y sistemas de información". Buenos Aires: Banco Central de la República Argentina. Obtenido de Banco Central de la República Argentina: http://www.bcra.gov.ar/pdfs/comytexord/A4609.pdf

López, P., Moya, F., Marimón, S., & Planas, I. (2011). *Protección de datos de salud. Criterios y plan de seguridad.* Madrid: Diaz de Santos.

International Organization for Standardization / International Electrotechnical Commission. (2013). *27002.* Suiza: ISO.

Peso Navarro, E. d., Ramos, M. A., & Peso, M. d. (2004). *El documento de Seguridad (Análisis Técnico y Jurídico. Modelo).* Madrid: Diaz de Santos.

Sallis, E., Caracciolo, C., & Rodriguez, M. (2010). *Ethical Hacking - Un enfoque metodológico para profesionales.* Buenos Aires: Alfaomega Grupo Editor.