XXXV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. CGCE, Buenos Aires, 2023.

Análisis de los cambios en los controles tecnológicos de la Comunicación A 7724 del BCRA en las entidades financieras.

Diego Sebastian Escobar.

Cita:

Diego Sebastian Escobar (2023). *Análisis de los cambios en los controles tecnológicos de la Comunicación A 7724 del BCRA en las entidades financieras. XXXV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. CGCE, Buenos Aires.*

Dirección estable: https://www.aacademica.org/escobards/71

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

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

Título: **"Análisis de los cambios en los controles tecnológicos de la Comunicación A "7724" del BCRA en las entidades financieras"**

Área: Contabilidad y Auditoría

Autor: ***Diego Sebastián Escobar***

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

Tabla de contenido

Análisis de los cambios en los controles tecnológicos de la Comunicación A 7724 del BCRA en las entidades financieras

1.1. Introducción

En el marco de las XXXV 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 los cambios en los controles tecnológicos de la Comunicación A “7724” del BCRA en las entidades financieras.

El objetivo de este trabajo es identificar los principales cambios señalados en la norma mencionada que deben tenerse en cuenta en los controles sobre tecnología y seguridad de la información de las entidades reguladas por el BCRA.

1.2. Características de la Comunicación A 7724

La comunicación del BCRA entró en vigencia en el año 2023, lo que representó un desafío en su implementación para las entidades financieras.

El texto ordenado cuenta con las siguientes secciones detalladas en el siguiente esquema:

Esquema N°1: Secciones de la Comunicación A 7724.

Fuente: BCRA Comunicación A 7724

1.3. Principales cambios en los controles tecnológicos y de Seguridad de la información

A continuación se detallan los principales conceptos incorporados:

1.3.1. Gobierno de TI y SI

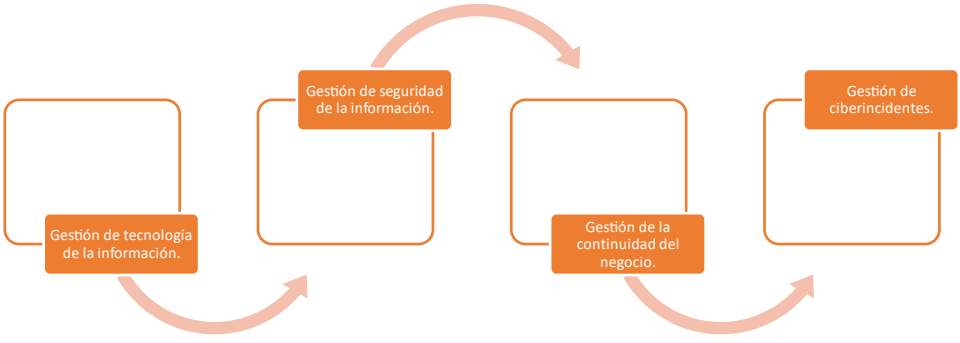
El concepto de Gobierno de Tecnología y Seguridad de la Información se refiere a "*un marco de trabajo integral que abarca las políticas, los procesos y los controles utilizados por las organizaciones para garantizar que la tecnología de la información (TI) y los sistemas de información se gestionen de manera efectiva y segura en línea con los objetivos y las normativas de la empresa*".

En particular, el Gobierno de Tecnología y Seguridad de la Información se enfoca en la gestión de riesgos, el cumplimiento normativo y la seguridad de la información en el entorno tecnológico. Esto implica la implementación de controles y prácticas para proteger la confidencialidad, integridad y disponibilidad de la información, al tiempo que se cumple con las regulaciones y normativas pertinentes en el ámbito de la seguridad de la información.

1.3.2. Marcos de Gestión

Las organizaciones financieras tienen que normalizar y publicar internamente los siguientes marcos de gestión:

Esquema N°2: Marcos de gestión



1.3.3. Nuevas responsabilidades del directorio y la alta gerencia

En la norma se establecieron las siguientes responsabilidades para el directorio y la alta gerencia:

Responsabilidades del directorio
Establecer y mantener componentes de gobierno coordinados con respecto a la autoridad y las responsabilidades para lograr la misión, las metas y los objetivos del negocio.
Aprobar y supervisar las estructuras organizacionales y las políticas de alto nivel relacionadas con el marco de gobierno de la tecnología y seguridad de la información.
Monitorear de manera continua el desempeño del gobierno de la tecnología y seguridad de la información, a fin de cumplir con las metas y objetivos establecidos.
Impulsar y supervisar los proyectos estratégicos de tecnología y seguridad de la información.
Asegurar la disposición de recursos adecuados y suficientes a las áreas relacionadas con la gestión de tecnología y la seguridad de la información.
Aprobar y supervisar el marco de gestión de riesgos, y el apetito de riesgo de tecnología de la información.
Fomentar una cultura de gestión de los riesgos de tecnología y seguridad de la información que abarque a toda la entidad.
Promover la implementación de un marco de gestión de seguridad de la información y supervisar su efectividad.
Aprobar el marco de gestión de continuidad del negocio y los mecanismos que aseguren la ciberresiliencia, y supervisar su desempeño.
Aprobar las políticas para gestionar la relación con terceras partes.
Aprobar las políticas para informar ciberincidentes significativos a las agencias gubernamentales.
Aprobar políticas para informar acerca de los incidentes que comprometan datos de clientes.
Fuente: BCRA Comunicación A 7724

Responsabilidades de la alta Gerencia

• **Diseñar estrategias y planes de tecnología de la información y definir el presupuesto necesario para cumplirlos.**
• **Conocer y comprender los riesgos relacionados con tecnología y seguridad de la informa- ción, asegurar que sean contemplados en los programas de gestión establecidos y definir planes de mitigación de los riesgos detectados.**
• **Diseñar estrategias, planes y medidas de seguridad de la información, y definir el presupuesto necesario para cumplirlos.**
• **Definir y asegurar la implementación y el mantenimiento de políticas de alto nivel.**
• **Definir los roles y responsabilidades necesarios para los procesos de tecnología y seguridad de la información de manera coordinada y eficaz.**
• **Establecer un marco de gestión de la seguridad de la información que permita asegurar la identificación, prevención, detección, respuesta y recuperación ante ciberincidentes.**
• **Implementar las prácticas de control interno y gestión de riesgos, y garantizar que las decisiones de tecnología de la información se tomen de acuerdo con el apetito de riesgo de la entidad.**
• **Delinear un marco de gestión de continuidad del negocio, sus documentos asociados y los informes resultantes.**
• **Definir e implementar un esquema de control y monitoreo continuo de los procesos, servicios y/o actividades delegadas en las terceras partes.**
• **Asegurar la gestión de los conocimientos, habilidades y capacidades de acuerdo con las tecnologías utilizadas.**
• **Establecer mecanismos de comunicación y coordinación entre las áreas de gestión de riesgos, tecnología y seguridad de la información para el cumplimiento de sus objetivos.**
• **Asegurar la incorporación en los proyectos de tecnología de la información el principio de seguridad desde el diseño.**
• **Asegurar la realización de evaluaciones de impacto y definición de apetitos de riesgo para la utilización de inteligencia artificial.**
• **Aprobar los protocolos de comunicación y las responsabilidades ante situaciones de escenarios de crisis y/o emergencia.**
• **Asegurar que los requerimientos vinculados a la protección de los usuarios de servicios financieros sean contemplados en los procesos de tecnología correspondientes.**
• **Aceptar los riesgos residuales derivados de la gestión de riesgos de tecnología y seguridad**
Fuente: BCRA Comunicación A 7724

1.4. Reflexiones finales

Los cambios recientes en los controles tecnológicos y de seguridad de la información se han centrado en la integración del concepto de Gobierno de Tecnología y Seguridad de la Información.

Este enfoque abarca políticas, procesos y controles diseñados para garantizar la gestión efectiva y segura de la tecnología de la información y los sistemas de información, priorizando la protección de la confidencialidad, integridad y disponibilidad de los datos.

Otra novedad importante radica en la integración de Marcos de Gestión en el contexto de las organizaciones financieras. Estas entidades están obligadas a establecer y divulgar internamente diversos marcos de gestión, incluyendo la gestión de tecnología de la información, seguridad de la información, continuidad del negocio y la de ciberincidentes. Esta medida busca estandarizar y fortalecer las prácticas de gestión en áreas críticas de las operaciones financieras.

En el marco de estas actualizaciones, se han establecido claramente responsabilidades específicas para el directorio y la alta gerencia. Se espera que estos actores clave desempeñen un papel activo en la implementación y el cumplimiento de los controles y prácticas de seguridad de la información. Esto implica una participación directa en la supervisión de las actividades de gobierno, así como un compromiso continuo con la mejora de los procesos y la mitigación de riesgos relacionados con la tecnología y la seguridad de la información.

1.5. Bibliografía

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. *Comunicación "A" 7724: "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

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.

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.

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. (2011). INCLUSIÓN DE CONCEPTOS BÁSICOS DE SEGURIDAD DE LA INFORMACIÓN EN LA FORMACIÓN DEL CONTADOR PÚBLICO. XXXIII Simposio Nacional de Profesores de Práctica Profesional. Universidad de La Plata, La Plata.

Escobar, D. S. (2011). La seguridad de la información y su contribución a la contabilidad. Mesa de Ciencias de la Secretaría de Investigación y Doctorado, Rumbo al Centenario 1913-2013. Secretaría de Investigación y Doctorado, FCE, UBA, Ciudad Autónoma de 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. (Trabajo Final de Posgrado. Universidad de Buenos Aires.) Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0817_EscobarDS.pdf

Escobar, D. S. (2017). Ciberseguridad documental de los sistemas contables legales. XI Congreso Internacional de Economía y Gestión. UBA, CABA.

Escobar, D. S. (2017). Concientización y capacitación del educando en la criticidad de la información contable en el ámbito de la práctica profesional. XXXIX SIMPOSIO DE PROFESORES DE PRÁCTICA PROFESIONAL. UNIVERSIDAD NACIONAL DE CATAMARCA, San Fernando del Valle de Catamarca.

Escobar, D. S. (2017). Formación del contador público en tecnología y seguridad de la información: Propuesta de reforma curricular. (Trabajo Final de Posgrado. Universidad de Buenos Aires.) Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1116_EscobarDS.pdf

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.

Escobar, D. S. (2019). Repensando la seguridad de los registros contables. I jornada de Ciberseguridad del Consejo Profesional en Ciencias Económicas. Consejo Profesional en Ciencias Económicas, CABA.

Escobar, D. S. (2022). Análisis de los modelos de gestión de Ciberseguridad en la elaboración de planes de concientización y capacitación para Contadores Públicos. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, (2-5), 1-7.

Escobar, D. S. (2022). Capacitación y concientización en seguridad de la información. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, (2-2), 1-6.

Escobar, D. S. (2022). El rol del Contador en la era digital. VI Jornadas de Orientación Vocacional. UBA, Buenos Aires.

Escobar, D. S. (2022). Identificación de los elementos para la descripción de un Modelo contable alternativo para el tratamiento de los activos de información. Sexta Jornada de Investigación Contable, Ética e Innovación: La Obra de Carlos Luis García Casella. Universidad de Buenos Aires - Facultad de Ciencias Económicas, Buenos Aires.

Escobar, D. S. (2022). Identificación de los elementos para la descripción de un Modelo contable alternativo para el tratamiento de los activos de información. Sexta Jornada de Investigación Contable, Ética e Innovación: La Obra de Carlos Luis García Casella. Universidad de Buenos Aires - Facultad de Ciencias Económicas, Buenos Aires.

Escobar, D. S. (2022). Identificación de los riesgos de los registros contables alojados en servicios de computación en la nube. XLIII Simposio Nacional de Profesores de Práctica Profesional. UNCUYO, Mendoza.

Escobar, D. S. (2022). Propuesta de un modelo contable que refleje el carácter de activo que la información corporativa representa para una entidad bancaria. (Tesis de Doctorado. Universidad de Buenos Aires.) Recuperado de http://bibliotecadigital.econ.uba.ar/download/tesis/1501-1323_EscobarDS.pdf

Escobar, D. S. (2022). Universo o dominio del discurso contable de los activos de información. ECON 2022. UBA, 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.