Exposición de trabajos en la Cátedra de Tecnología Aplicada a la Información Contable. MCI - Cátedra de Tecnología Aplicada a la Información Contable, Buenos Aires, 2025.

# Hashes criptográficos en el contexto de la seguridad de la información y su aplicación en las PyMEs argentinas.

CARLOS LUIS PACINI , LUCIANA MARIA RIOS, MELINA SOLEDAD MISKOW y PAULA IVANA DIEZ .

Cita:

CARLOS LUIS PACINI , LUCIANA MARIA RIOS, MELINA SOLEDAD MISKOW y PAULA IVANA DIEZ (2025). *Hashes criptográficos en el contexto de la seguridad de la información y su aplicación en las PyMEs argentinas. Exposición de trabajos en la Cátedra de Tecnología Aplicada a la Información Contable. MCI - Cátedra de Tecnología Aplicada a la Información Contable, Buenos Aires.*

Dirección estable:
https://www.aacademica.org/mci.catedra.de.tecnologia.aplicada.a.la.informacion.contable/14

ARK: https://n2t.net/ark:/13683/pYAR/1On

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Negocios y Administración Pública

TECNOLOGÍA APLICADA A LA INFORMACIÓN CONTABLE

# Hashes criptográficos en el contexto de la seguridad de la información y su aplicación en las PyMEs argentinas

ALUMNOS:

- CARLOS LUIS PACINI 03pa30572042@campus.economicas.uba.ar
- LUCIANA MARIA RIOS 42ri36572218@campus.economicas.uba.ar
- MELINA SOLEDAD MISKOW 02mi42874973@campus.economicas.uba.ar
- PAULA IVANA DIEZ 36di27702412@campus.economicas.uba.ar

POSGRADO: MAESTRÍA EN CONTABILIDAD INTERNACIONAL

DESCRIPCIÓN BREVE: En este trabajo se define y se explica la utilidad de la aplicación de funciones hash en PyMEs con el objeto de preservar la integridad de la información, entendiendo este recurso como amigable al usuario no experto considerando que este tipo de organizaciones no siempre cuentan con personal especializado en ciberseguridad.

PALABRAS CLAVES: PYMES, HASH, CIBERSEGURIDAD, ARGENTINA, TECNOLOGÍA DE LA INFORMACIÓN

6 DE AGOSTO DE 2025

# INDICE

# INTRODUCCIÓN

Las Pequeñas y Medianas Empresas (PyMES) son actores muy relevantes para la economía y la sociedad argentina ya que representan el 99,4% de las empresas en Argentina y generan el 66% de la fuerza laboral privada, siendo clave en sectores como servicios, comercio, industria y agropecuario, según datos de la Secretaría de Industria y Desarrollo Productivo (2023).

Entre los desafíos que enfrentan las PyMES podemos mencionar: falta de financiamiento, inflación, dificultades para escalar tecnológicamente o exportar y una creciente digitalización que las expone a ciberataques. A nivel mundial, el Foro Económico Mundial también sostiene que las PyMES se enfrenan a retos de ciberseguridad por sus limitaciones presupuestarias, el escaso conocimiento de las amenazas y protocolos de seguridad insuficientes, entre otros.

Las PyMES argentinas de tamaño medio (100-250 empleados) destinan un 24% de su presupuesto de TI a ciberseguridad, más que el promedio regional (16,5%). Sin embargo, esta inversión suele ser reactiva, no proactiva, lo que limita su efectividad y pone de manifiesto la necesidad de medidas de seguridad robustas.

# HASHES CRIPTOGRÁFICOS EN EL CONTEXTO DE LA SEGURIDAD DE LA INFORMACIÓN - RELACIÓN CON LAS PyMEs ARGENTINAS

## 1. CONTEXTO DE LAS PyMES EN ARGENTINA Y LA CIBERSEGURIDAD

Considerando que las PyMES son blanco de ataques como ransomware y phishing, es necesario que formulen una estrategia de ciberseguridad integral más allá del uso de hashes.

Sin perjuicio de lo anteriormente manifestado, en este trabajo nos enfocaremos en mostrar como una PyME que carece de personal capacitado en ciberseguridad - lo que dificultaría en principio la implementación efectiva de funciones hash - podría implementar y llevar un sistema de hashes para garantizar la integridad, autenticidad y confidencialidad de la información que genera y maneja.

## 2. ¿QUÉ ES UN HASH CRIPTOGRÁFICO Y CUAL ES SU RELEVANCIA EN SEGURIDAD?

Un hash criptográfico es un código alfanumérico de longitud fija generado por una función hash a partir de datos de cualquier tamaño y tipo (texto, archivos PDF, carpetas con archivos, hojas de cálculo, etc.).

Este código alfanumérico único funciona como una "huella digital" de un archivo. Si el documento se altera, por mínimo que sea el cambio, su hash cambiará.

Las características claves de los hashes son:

- Determinismo: El mismo dato siempre genera el mismo hash.

- Irreversibilidad: No se puede reconstruir el dato original a partir del hash.
- Sensibilidad a cambios: Cualquier modificación en el dato produce un hash completamente diferente.
- Resistencia a colisiones: Es extremadamente difícil encontrar dos datos distintos que generen el mismo hash.

Estas propiedades hacen que los hashes sean fundamentales para garantizar la integridad, autenticidad y confidencialidad de la información en aplicaciones como:

- Verificación de integridad de archivos (Por ejemplo: descargas seguras).
- Almacenamiento seguro de contraseñas.
- Firmas digitales y certificados SSL/TLS.
- Seguridad en blockchain y criptomonedas.

## 3. USO DE HASHES CRIPTOGRÁFICOS EN PyMES ARGENTINAS

Los usos más usuales de hashes criptográficos por parte de las PyMES argentinas, basándonos en el contexto de ciberseguridad y las tecnologías emergentes, son:

a) Protección de datos sensibles:

- Almacenamiento de contraseñas: las PyMES que manejan datos de clientes (ej. comercio electrónico, servicios financieros) usan funciones hash para almacenar contraseñas de forma segura, evitando guardarlas en texto plano. Esto protege contra accesos no autorizados.
- Integridad de datos: las PyMES que intercambian archivos (ej. contratos, facturas) pueden usar hashes para verificar que no han sido alterados durante la transmisión.

b) Firmas digitales y certificados: las PyMES que operan en comercio electrónico o firman contratos digitales usan hashes en firmas electrónicas para garantizar la autenticidad e integridad de los documentos. Los certificados SSL/TLS, esenciales para sitios web de PyMES (por ejemplo, facturación electrónica), dependen de funciones hash para proteger transacciones en línea.

c) Detección de malware: las PyMEs que implementan software antivirus utilizan bases de datos de hashes para identificar malware, comparando los hashes de archivos con firmas de códigos maliciosos conocidas.

d) Blockchain y criptoactivos: algunas PyMES argentinas, especialmente en el sector Fintech, están explorando tecnologías de blockchain (DLT) para financiamiento o transacciones. Los hashes son fundamentales en blockchain para garantizar la integridad de las transacciones y evitar manipulaciones. Por ejemplo, Blockchain Federal Argentina destaca que los hashes permiten verificar cambios en documentos sin almacenar los datos originales.

## 4. BENEFICIOS DE LOS HASHES PARA LAS PyMES ARGENTINAS

- Seguridad a bajo costo: los algoritmos hash son gratuitos y ampliamente disponibles, lo que los hace accesibles para PyMES con presupuestos limitados.
- Confianza del cliente: al proteger datos sensibles (contraseñas, transacciones), las PyMES pueden generar confianza en sus clientes.
- Cumplimiento normativo: el uso de hashes en firmas digitales y certificados ayuda a cumplir con regulaciones locales e internacionales.
- Integridad en transacciones: los hashes aseguran que los datos no se alteren, lo cual es crucial para PyMES que operan en mercados digitales o exportan.

## 5. LIMITACIONES

Básicamente referidas a las vulnerabilidades de algoritmos obsoletos: algoritmos como MD5 y SHA-1 son ahora inseguros debido a colisiones; las PyMES deben utilizar SHA-256 o SHA-3.

El proceso de hashing puede ser computacionalmente intensivo, especialmente con grandes volúmenes de datos.

Se requiere que las empresas combinen la generación de hashes con otras medidas de seguridad para mitigar riesgos.

## 6. CASO DE APLICACIÓN

El uso de hashes es una práctica sencilla para añadir una capa de seguridad y control sobre la documentación importante de una PyME, garantizando su autenticidad a lo largo del tiempo.

Para aplicar un hash a los documentos generados en una PyME se pueden utilizar programas sencillos y en su mayoría gratuitos. Este proceso garantiza la integridad de los archivos, asegurando que no han sido modificados.

### 6.1. ¿Cómo se aplica el hash a un documento?

El proceso es simple y no requiere conocimientos técnicos avanzados:

1) Instalar un programa o software para generar hashes.
2) Seleccionar el archivo: se abre el programa instalado previamente y se selecciona el documento (PDF, Word, Excel, etc.) al que se quiere aplicar el hash.
3) Generar el hash: el software procesará el archivo y mostrará su código hash (es recomendable usar el algoritmo SHA-256, que es un estándar seguro y muy utilizado).

4) Guardar el hash: se copia y guarda este código alfanumérico junto a una referencia del documento. Se puede guardar en un archivo de texto, una planilla de excel, o en el sistema de gestión de la empresa.

De esta forma, si en el futuro se necesita verificar que un documento es el original, simplemente se vuelve a calcular su hash y se lo compara con el que se ha guardado previamente. Si coinciden, el archivo está intacto.

## 6.2. Programas para generar hash

Para el uso en PyMEs, se puede optar por herramientas modernas, versátiles y fáciles de usar. Algunas de las mejores opciones gratuitas son:


Es una de las opciones más populares. Se integra directamente en el menú de "Propiedades" de cualquier archivo. Solo se debe hacer click derecho sobre el documento, ir a Propiedades y se encontrará una nueva pestaña llamada "Hashes de archivo" donde se encuentran los códigos en diferentes algoritmos (MD5, SHA-1, SHA-256, etc.).


Es una herramienta liviana y portable (no requiere instalación). Te permite calcular el hash de múltiples archivos a la vez, arrastrándolos y soltándolos en su ventana. Es ideal para procesar lotes de documentos.

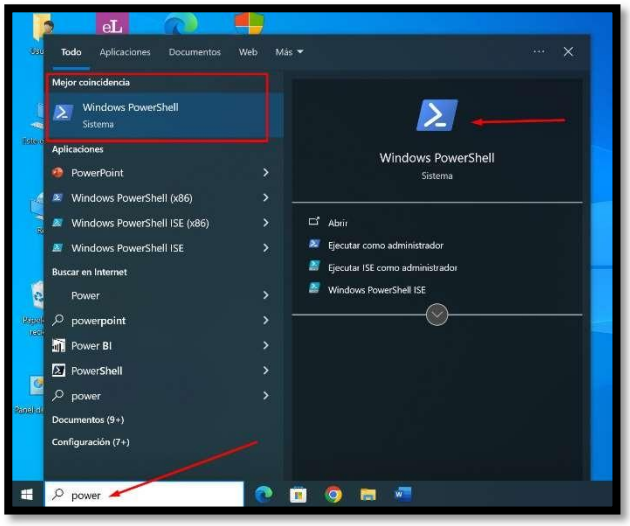

Una opción muy completa y de código abierto. Funciona en Windows, macOS y Linux. Ofrece funciones avanzadas, como hashear carpetas enteras o incluso comparar archivos.

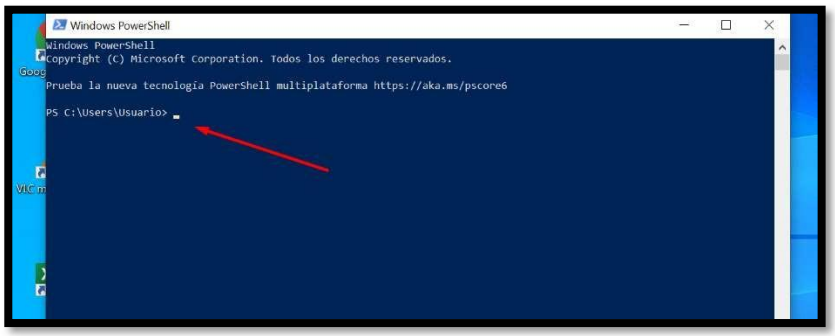
## 6.3 Integrado en Windows

También se puede usar una herramienta que ya viene con Windows, sin necesidad de instalar nada adicional. Teniendo en cuenta que en casi la totalidad de las PyMES argentinas se utiliza Windows, vamos a demostrar su aplicación práctica.

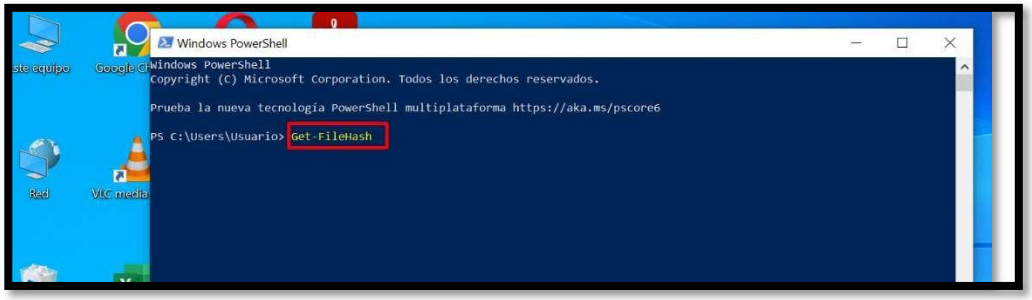
- PowerShell:

1) Abrir PowerShell (se accede mediante el menú de inicio).

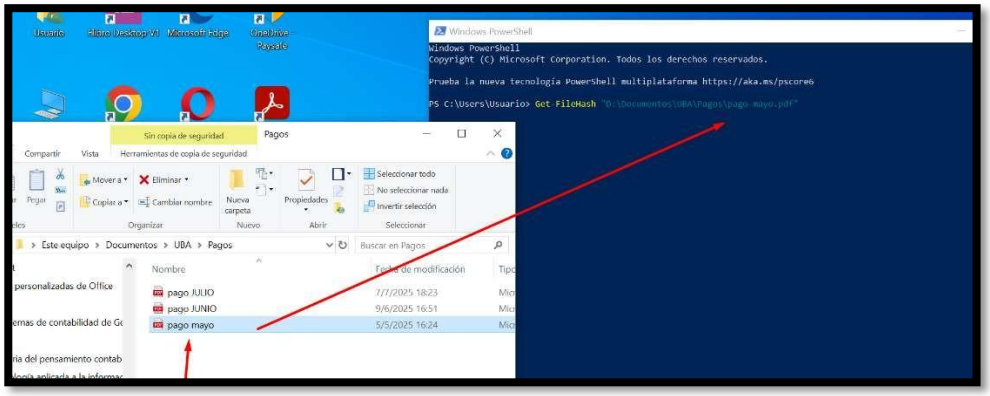


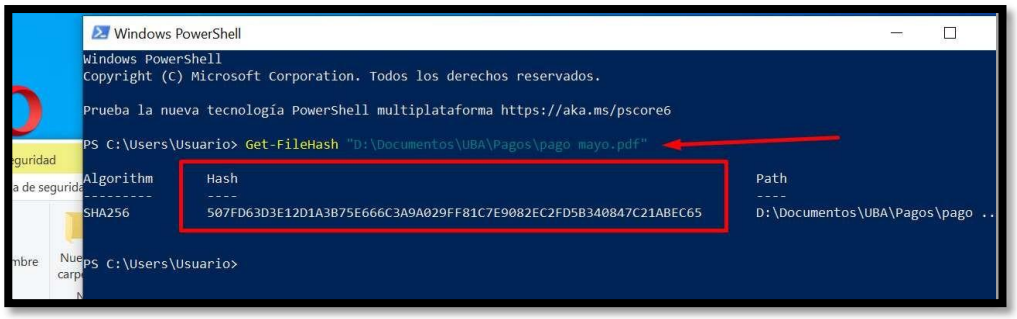

2) Escribir el comando Get-FileHash seguido de un espacio (se puede copiar y pegar).




3) Se arrastra el archivo que se quiere hashear desde la carpeta donde está ubicado hasta la ventana de PowerShell (la ruta del archivo se pegará automáticamente).



4) Se presiona Enter y el programa te mostrará el hash SHA-256 calculado para ese documento.




5) Una vez que el programa te muestra el código hash, no se inserta ni se vincula técnicamente al archivo original. Hacerlo modificaría el archivo y, por lo tanto, cambiaría su propio hash, invalidando el proceso.

Lo que se debe hacer es guardar ese código hash por separado como un registro de control. Se piensa el hash como el número de serie único del documento procesado en un momento específico. Se debe anotar ese número de serie en un lugar seguro.

Una forma práctica y sencilla de hacerlo en una PyME es llevar un registro en una planilla de cálculo: pensamos que es la forma más ordenada y escalable.

- Se crea una planilla en Excel o en Google Sheets.
- Se designan columnas para la información clave.
- Por cada documento al que se le genera un hash se completa una fila.

Ejemplo de registro de hashes en una PyME (Estudio Contable):

| Nombre del Archivo | Fecha de Generación | Hash SHA-256 | Responsable | Notas |
|---|---|---|---|---|
| Contrato_Servicios_Aprendiendo SRL.pdf | 16/3/2025 | a3f...d9b | Cdra. Paula Diez | Versión final firmada |
| EEFF_Maestría SA_Mayo2025.xlsx | 1/8/2025 | e1c...74a | Cdra. Melina Miskow | Presentado a gerencia |
| DDJJ_IVA_06_2025_Aprendiendo SRL.pdf | 22/7/2025 | 55d...82f | Cdr. Carlos Pacini | Versión presentada ARCA |
| DDJJ_Ganancias_2024_Diego Escobar.pdf | 20/6/2025 | 71x...jp9 | Cdra. Luciana Ríos | Versión final firmada por el cliente |

Ventajas de este método de guarda de los hashes:

- Centralizado: toda la información de integridad está en un solo lugar.
- Ordenado: fácil de buscar y filtrar.
- Seguro: se puede proteger con contraseña la planilla.

Otra opción más simple aún para archivos individuales:

- Generar el hash del documento, por ejemplo, Factura_001.pdf.
- Copiar el código hash.
- Crear un nuevo archivo de texto (.txt).
- Se pega el hash dentro y se guarda el archivo con un nombre similar, como Factura_001.pdf.hash.txt.
- Se guardan ambos archivos (el original y su .txt con el hash) en la misma carpeta.

6) ¿Cómo verifico la integridad del documento después? El proceso es el inverso:

1. Se busca el hash original en la planilla de cálculo.
2. Se calcula el hash actual del documento con el programa utilizado para generar el hash anteriormente.
3. Se compara:

 Si el nuevo hash es idéntico al que está guardado en la planilla, se tiene la certeza matemática de que el archivo no ha sufrido ninguna alteración.

 Si el nuevo hash es diferente, aunque sea por un solo carácter, el archivo fue modificado, guardado de nuevo o está corrupto. 🚩

 Se puede verificar esto con una simple fórmula de Excel:

| | A | B | C | D | E |
|---|---|---|---|---|---|
| | ***Hash original*** | 507FD63D3E12D1A3B75E666C3A9A029FF81C7E9082EC2FD5B340847C21ABEC65 | | | |
| | ***Hash del documento sin cambios*** | 507FD63D3E12D1A3B75E666C3A9A029FF81C7E9082EC2FD5B340847C21ABEC65 | | VERDADERO | =+B4=B2 |
| | ***Hash del documento con cambios*** | 888D081717463D2DDD586233C9BCD82BA742EE7AF1DAD749B0F0CA83DDDC4C21 | | FALSO | =+B2=B6 |

Como hemos visto, la vinculación no es técnica, sino de registro y procedimiento:

 Se guarda el hash como una prueba testigo en un lugar seguro y se usa para comparar en el futuro.

7) Escalabilidad:

Este procedimiento que hemos realizado con un archivo individual es posible automatizarlo para procesar un mayor número de archivos mediante la ejecución de un código de PowerShell.

La automatización mediante script consiste en que la aplicación ubique la carpeta (o carpetas) indicada a una hora preestablecida, que calcule los hashes de todos los archivos nuevos que se fueron almacenando durante el día en la carpeta y que los guarde en un archivo txt o excel de registros.

De esta forma no se requiere la afectación de horas de empleados para ejecutar la tarea, reduciendo a cero el costo de implementación y evitando la reticencia al cambio.

Por otra parte, si posteriormente se necesita controlar la integridad de los archivos, es decir, si se quiere saber si los documentos almacenados sufrieron cambios desde la fecha en que se archivaron y la fecha posterior en la que se precisan utilizar, se puede ejecutar otro script para que el programa realice el cálculo de todos los hashes nuevamente y los compare con los hashes guardados en el txt indicando archivo por archivo si coincide con el hash original o si cambió.

# CONCLUSIÓN

Desde hace varios años se vive en un mundo globalizado, donde los ataques informáticos son más recurrentes para todos pero en específico para las PyMES que en su mayoría no cuentan con personal especializado o con el suficiente conocimiento para prevenirlos. Es por ello que las PyMES argentinas, aún con las limitaciones que enfrentan, pueden adoptar hashes criptográficos para proteger datos sensibles, garantizar la integridad de transacciones y cumplir con normativas.

Los hashes, al ser herramientas accesibles y efectivas, representan una oportunidad para que las PyMES fortalezcan su seguridad digital.

Dada nuestra experiencia laboral con clientes titulares de PyMEs y empresas unipersonales, podemos ver en ellos una resistencia al cambio y a la adopción de estas nuevas tecnologías, especialmente en aquellos que ya están acostumbrados a los procesos tradicionales, impulsando al profesional contable a interpretar el papel de intermediario y también maestro en estos temas, para ayudarlos en la transición hacia la digitalización de una forma amena y sencilla.

Actualmente se utilizan los hashes en ciertos procedimientos de liquidaciones de impuestos (por ejemplo en las DDJJ de Agentes de Recaudación de Ingresos Brutos de ARBA) y vemos viable la posibilidad de extender el uso del hash criptográfico hacia otras áreas de las PyMEs, de modo que puedan llevar, por ejemplo, un registro de su documentación hasheado para preservar la integridad de la información.

Hoy en día las Pymes brindan una gran oportunidad de desarrollo al profesional, hay mucho por hacer y existen herramientas disponibles que pueden implementarse que antes eran exclusivas de las grandes empresas. El contador tiene la posibilidad de convertirse en un asesor capacitado y realizar un trabajo de asesoramiento útil para la empresa que encara un proyecto de TI.

## BIBLIOGRAFIA


World Economic Forum (2024) Como pueden las pymes convertir el riesgo de ciberseguridad en una oportunidad. Recuperado de https://es.weforum.org/stories/2024/08/las-pymes-puedenconvertir-el-riesgo-de-ciberseguridad-en-una-oportunidad-como-hacerlo/

Secretaría de la Pequeña y Mediana Empresa, Emprendedores y Economía del Conocimiento. (2024). Estadísticas de PyMEs, Emprendedores y Economía del Conocimiento: estado de situación a diciembre de 2023 (Informe elaborado en diciembre de 2024). Ministerio de Economía. Recuperado de: https://www.argentina.gob.ar/sites/default/files/informe_2023_nov_2024.pdf

Blockchain Federal Argentina. (s. f.). Blockchain Federal Argentina. Recuperado de https://bfa.ar/

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.

Schneider, J. (2024). Casos de uso de la criptografía: de la comunicación segura a la seguridad de datos.

IBM. Recuperado de https://www.ibm.com/eses/think/topics/cryptography-use-caseschrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mpf.gob.ar/ufeci/files/2023/05/Informe_Criptoactivos.pdf

FasterCapital. (s.f.). Casos de uso práctico de funciones hash en criptografía. Recuperado de https://fastercapital.com/es/tema/casos-de-uso-pr%C3%A1ctico-de-funciones-hash-encriptograf%C3%ADa.html/1

Latin Pyme (2025) 1 de cada 5 PyMEs en Latinoamérica expone su seguridad digital por falta de expertos. Recuperado de https://latinpyme.com/1-de-cada-5-pymes-en-latinoamericaexpone-su-seguridad-digital-por-falta-de-expertos/

Prof. Mg. Daniel Piorun, El contador frente al paradigma de la transformación digital de las organizaciones, Enfoques (Mayo 2018), Thomson Reuters