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.

PRINCIPALES RETOS EN SEGURIDAD Y PREVENCION DE FRAUDES.

María Florencia Parella, Martín Goñi y Luz Sanchez.

Cita:

María Florencia Parella, Martín Goñi y Luz Sanchez (2025). *PRINCIPALES RETOS EN SEGURIDAD Y PREVENCION DE FRAUDES. 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/13

ARK: https://n2t.net/ark:/13683/pYAR/HSA

TECNOLOGIA APLICADA A LA INFORMACION CONTABLE

PRINCIPALES RETOS EN SEGURIDAD Y PREVENCION DE FRAUDES

Maestrandos:

María Florencia Parella (florencia.parrella@gmail.com)
Luz Sanchez (marialuzsanchez14@gmail.com)
Martín Goñi (martingonig@gmail.com)

RESUMEN: El trabajo analiza el papel de la auditoría externa en la evaluación de controles de seguridad informática, destacando herramientas como auditorías técnicas, pruebas de penetración y análisis de vulnerabilidades. Se abordan los riesgos asociados a la transformación digital y se proponen buenas prácticas para prevenir fraudes y mejorar la ciberseguridad en entornos contables.

PALABRAS CLAVES: Auditoría externa, ciberseguridad, prevención de fraudes, vulnerabilidades, sistemas contables.

INTRODUCCION

En la actualidad, la transformación digital ha revolucionado los procesos organizacionales, especialmente aquellos relacionados con la gestión financiera y contable. Sin embargo, este avance tecnológico también ha traído consigo un aumento en la frecuencia y sofisticación de los ataques cibernéticos, lo que representa un riesgo creciente para la integridad, disponibilidad y confidencialidad de la información. Ante esta realidad, las organizaciones deben implementar controles de seguridad sólidos que les permitan proteger sus activos digitales, garantizar la continuidad operativa y mantener la confianza de sus grupos de interés.

En este contexto, la auditoría externa adquiere un papel estratégico al evaluar la existencia, eficacia y adecuación de los controles de seguridad implementados por la entidad. Esta evaluación implica revisar si la organización cuenta con políticas claras, procedimientos bien definidos y tecnologías apropiadas para mitigar los riesgos derivados de posibles vectores de ingreso no autorizados o ataques maliciosos. La auditoría no solo verifica el cumplimiento normativo y la gestión de riesgos, sino que también contribuye a fortalecer el control interno y la transparencia de los procesos.

Este trabajo tiene como objetivo analizar el papel de la auditoría externa en la evaluación de los controles de seguridad dentro de una organización, con énfasis en su capacidad para detectar deficiencias, prevenir incidentes y formular recomendaciones que mejoren la postura de seguridad. La naturaleza del estudio es analítica y exploratoria, ya que busca comprender las implicaciones que tiene esta evaluación en el ámbito contable, tecnológico y operativo de las empresas.

El propósito de este análisis es ofrecer una visión clara y fundamentada sobre cómo la auditoría externa puede convertirse en un mecanismo eficaz de prevención y mejora continua frente a los riesgos tecnológicos. Sus aplicaciones son especialmente relevantes en sectores que manejan información financiera sensible, como la banca, las aseguradoras, las entidades gubernamentales y cualquier organización que deba cumplir con estándares de seguridad y normativas internacionales.

DESARROLLO

¿Qué es una auditoría de seguridad informática?

Es una evaluación que se realiza en las empresas para determinar el estado o nivel de la ciberseguridad de los sistemas informáticos, el acceso a internet, las políticas de seguridad y su cumplimiento por parte del personal. Estas auditorías pueden ser técnicas, es decir, pruebas realizadas por expertos en

ciberseguridad en donde se analizan las vulnerabilidades; pueden ser una revisión de controles ante una autoridad, como por ejemplo para las certificaciones ISO 27001 y PCI-DSS.

Al realizar este tipo de evaluaciones, se busca entregar un informe final, en el cual se reporte los equipos, servidores y programas instalados que se analizaron, el cumplimiento de las normas de seguridad establecidas por la empresa, la eficiencia de los sistemas de seguridad y las posibles vulnerabilidades o brechas en cualquier nivel de seguridad de la empresa.

¿Cómo llevar a cabo pruebas de vulnerabilidades?

1. Auditorías técnicas

Son las que realiza un experto en seguridad informática, con el fin de evaluar el nivel de seguridad de los componentes técnicos del sistema, como activos de información. Las auditorías técnicas se basan en herramientas específicas para analizar y probar la seguridad técnica del sistema, como las pruebas de vulnerabilidad, las pruebas de penetración o el análisis forense. Las auditorías técnicas permiten identificar y solucionar las vulnerabilidades y las amenazas técnicas del sistema, así como que proporcionan una visión detallada y precisa del nivel de seguridad técnica del sistema.

2. Hacking ético o Pruebas de Penetración

En este caso, la práctica consiste en realizar pruebas de seguridad informática simulando los ataques informáticos o las amenazas que podrían sufrir la organización o el sistema por parte de agentes maliciosos, con el fin de identificar y solucionar las vulnerabilidades y debilidades existentes. Se basan en aplicar las técnicas y las herramientas propias del hacking, pero con fines legítimos y autorizados. Estas auditorías pueden incluir la realización de escaneos de vulnerabilidad, pruebas de penetración o pentesting, análisis de código, entre otros.

Nos enfocamos en el paso a paso de la prueba de penetración:

Paso 1: Reconocimiento

- Recopilar información pública del servidor: dominio, dirección IP, tecnologías usadas en el sitio web.

Paso 2: Escaneo de vulnerabilidades

- Usar un escáner como para detectar vulnerabilidades conocidas en el servidor y en el software del servidor web.

Paso 3: Análisis de vulnerabilidades

- Identificar si hay versiones desactualizadas de software, configuraciones débiles, o vulnerabilidades conocidas.

Paso 4: Explotación controlada

- Realizar pruebas para explotar alguna vulnerabilidad identificada, por ejemplo, manipular inyecciones SQL o explotar errores conocidos en la versión del servidor web.

Paso 5: Evaluación y reporte

- Documentar los hallazgos, explicar el riesgo asociado (por ejemplo, posible acceso no autorizado a datos), y recomendar soluciones como actualizaciones de software, configuraciones más seguras, o parches.

3. Análisis de Vulnerabilidad

El análisis de vulnerabilidades es un componente clave de cualquier estrategia eficaz de ciberseguridad. Implica procesos automatizados para detectar vulnerabilidades de software, sistemas y redes, lo que permite a las organizaciones corregir las brechas de seguridad antes de que los ciberdelincuentes las exploten. A medida que los ataques se vuelven más sofisticados, analizar periódicamente su entorno es esencial para proteger datos confidenciales, evitar filtraciones y cumplir con los requisitos normativos.

¿Qué buscar en un escáner de vulnerabilidades?

Al seleccionar un escáner de vulnerabilidades, una organización debe buscar características claves en la solución de software elegida. Las mismas son:

- **Cobertura integral (redes, aplicaciones, nube)**: las organizaciones deben priorizar las herramientas que ofrecen una cobertura integral en todo su entorno de TI, incluidas las redes, las aplicaciones y la infraestructura de la nube.

- **Escaneos con credenciales y sin credenciales**: la capacidad de realizar escaneos con credenciales y sin credenciales es esencial para identificar una amplia gama de vulnerabilidades, desde configuraciones incorrectas del sistema hasta fallas profundas en las aplicaciones.

- **Escalabilidad e integración**: la escalabilidad y la facilidad de integración con las herramientas de seguridad existentes también son fundamentales para garantizar que el escáner pueda crecer con las necesidades de la organización y adaptarse perfectamente a su ecosistema de ciberseguridad.

- **Actualizaciones oportunas y automatización**: un escáner de vulnerabilidades confiable también debe proporcionar actualizaciones oportunas para mantenerse a la vanguardia de las amenazas emergentes y ofrecer informes detallados y prácticos que ayuden a priorizar las vulnerabilidades en función de la gravedad y el riesgo.

- **Funciones de automatización**: La automatización es una función clave para los analizadores de vulnerabilidades. Les permite detectar y responder rápidamente a las vulnerabilidades, lo que ayuda a las organizaciones a reducir la intervención manual y a remediar los riesgos con mayor rapidez.

- **Informes detallados y prácticos**: los buenos escáneres de vulnerabilidad encuentran problemas y brindan informes detallados que ayudan a las organizaciones a priorizar las soluciones según la gravedad de las vulnerabilidades, el riesgo para las operaciones comerciales y los requisitos de cumplimiento.

- **Escaneo continuo y monitoreo en tiempo real**: algunos escáneres ofrecen capacidades de escaneo continuo, proporcionando monitoreo en tiempo real para detectar vulnerabilidades a medida que aparecen, lo que es cada vez más importante en entornos modernos y dinámicos.

La integración de auditorías de seguridad informática en el entorno contable no solo responde a una necesidad técnica, sino también estratégica. La detección proactiva de vulnerabilidades y la implementación de medidas correctivas oportunas permiten preservar la integridad de los datos financieros, asegurar la trazabilidad de la información y fortalecer el sistema de control interno. En un contexto donde la confianza es un activo clave, especialmente en sectores regulados o altamente expuestos como el financiero y el público, la auditoría externa actúa como un garante del cumplimiento normativo y de la transparencia. Así, la colaboración entre equipos técnicos, contables y auditoría se vuelve esencial para afrontar con éxito los desafíos de la era digital.

CONCLUSIONES

La creciente digitalización de los procesos contables y financieros ha expuesto a las organizaciones a nuevos y complejos riesgos en materia de seguridad informática. En este escenario, la auditoría externa se posiciona como una herramienta clave para evaluar y reforzar los controles existentes, contribuyendo a la prevención de incidentes y fraudes. A través de auditorías técnicas, pruebas de

penetración y análisis de vulnerabilidades, es posible identificar debilidades en los sistemas y proponer mejoras concretas.

La implementación de escáneres de vulnerabilidades eficaces, junto con procesos automatizados y monitoreo continuo, permite a las organizaciones anticiparse a posibles ataques, proteger información sensible y cumplir con los estándares normativos. Así, el rol del auditor externo trasciende la simple revisión documental, consolidándose como un actor estratégico en la construcción de entornos digitales más seguros, confiables y resilientes. Integrar estas prácticas en la gestión contable no solo fortalece el control interno, sino que también genera valor mediante la confianza que proyectan las organizaciones al garantizar la integridad de su información.

BIBLIOGRAFIA

- https://www.linkedin.com/pulse/auditor%C3%ADa-de-seguridad-inform%C3%A1ticatipos-fases-y-ventajas/
- https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/
- 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.