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.

Cyber Security 2.0.

MARIA SOLEDAD AUDIA, TOMÁS IDIART, PAOLA BURGOS HERNANDEZ, LEONARDO GIL JIMENEZ y AYLÉN VALLS.

Cita:

MARIA SOLEDAD AUDIA, TOMÁS IDIART, PAOLA BURGOS HERNANDEZ, LEONARDO GIL JIMENEZ y AYLÉN VALLS (2025). *Cyber Security 2.0. 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/17

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

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

MAESTRÍA EN CONTABILIDAD INTERNACIONAL

TECNOLOGÍA APLICADA A LA INFORMACIÓN CONTABLE

Título: Cyber Security 2.0

Trabajo Grupal - Final

AUTORES: MARIA SOLEDAD AUDIA, TOMÁS IDIART, PAOLA BURGOS HERNANDEZ, LEONARDO GIL JIMENEZ, AYLÉN VALLS

Agosto 2025

Tabla de contenido

Introducción

En un contexto donde la digitalización de los procesos empresariales es una condición necesaria para la competitividad, la protección de la información ha adquirido una relevancia estratégica. La creciente dependencia de los sistemas informáticos, la expansión del trabajo remoto y el uso intensivo de datos sensibles exponen a las organizaciones a múltiples riesgos vinculados a la ciberseguridad. Los ataques informáticos, como el malware, el phishing o la fuga de datos, ya no afectan solamente a grandes corporaciones, sino que impactan cada vez más a pequeñas y medianas empresas, generando pérdidas económicas, daños reputacionales y responsabilidades legales significativas (ISO/IEC, 2013).

En este escenario, la ciberseguridad deja de ser un asunto exclusivo del área de tecnología para convertirse en una dimensión transversal que exige la participación de todas las áreas organizacionales, incluyendo al ámbito contable. Tradicionalmente vinculado a los registros contables, al control financiero y la elaboración de estados contables, el contador enfrenta hoy el desafío de integrarse activamente en la gestión de riesgos digitales, velando por la integridad, confidencialidad y disponibilidad de la información financiera, operativa y estratégica.

El presente trabajo tiene como objetivo analizar el impacto de la ciberseguridad en las empresas y destacar el rol estratégico que el profesional contable asume en este nuevo contexto. Para ello, se abordarán los principales riesgos

asociados, las normas y buenas prácticas aplicables, y las competencias clave que requiere el ejercicio profesional ante las exigencias del entorno digital actual.

Desarrollo

Ciberseguridad, una necesidad

La ciberseguridad se refiere al conjunto de prácticas, procesos y tecnologías diseñadas para proteger los sistemas informáticos, redes, programas y bases de datos digitales frente a ataques, daños o accesos no autorizados. Si bien suele confundirse con el concepto de seguridad de la información, este último es más amplio, ya que incluye la protección de la información en todos sus formatos (digital, físico, verbal), no sólo la digital. Según la norma ISO/IEC 27001 "Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos", la seguridad de la información busca garantizar la confidencialidad, integridad y disponibilidad de los datos (ISO/IEC, 2013).

Complementariamente, la norma ISO/IEC 27032 "Ciberseguridad: Directrices para la seguridad en Internet" define el ciberespacio como "el entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos y redes interconectados", señalando la necesidad de proteger los activos digitales frente a amenazas internas y externas.

En la actualidad, las empresas enfrentan una variedad de amenazas cibernéticas que evolucionan constantemente. Algunas de las más comunes incluyen:

- Phishing: intentos de engaño para obtener credenciales o información confidencial (por ejemplo, contraseñas o datos bancarios) simulando ser una fuente confiable.
- Malware: programas que buscan dañar o acceder sin autorización a sistemas (troyanos, virus, spyware).
- Ransomware: tipo de malware que bloquea el acceso a sistemas o archivos hasta que se pague un rescate.
- Fuga o pérdida de datos: ya sea por errores humanos, negligencia o acciones maliciosas internas, los datos sensibles pueden ser expuestos.
- Suplantación de identidad (spoofing) y ataques de ingeniería social que explotan la confianza de los usuarios.

El impacto de los incidentes de ciberseguridad se manifiesta en múltiples dimensiones. En lo económico, los costos pueden incluir rescates pagados, inversiones en recuperación, pérdida de ingresos y sanciones. En lo legal, las organizaciones pueden enfrentar consecuencias derivadas del incumplimiento normativo, incluyendo responsabilidades penales bajo la Ley 27.401. En términos reputacionales, la pérdida de confianza por parte de clientes, proveedores y socios puede tener efectos a largo plazo, especialmente en un entorno cada vez más exigente con la gestión ética de la información.

Por estas razones, la ciberseguridad se ha convertido en un eje clave de la gestión empresarial moderna, y su abordaje ya no puede limitarse al área técnica, sino que debe involucrar activamente a todos los actores organizacionales, incluido el contador.

Marco legal

La ciberseguridad no puede gestionarse de forma aislada ni empírica: requiere apoyarse en normas técnicas reconocidas y en un marco legal que garantice la protección adecuada de los datos en las organizaciones. Tanto a nivel internacional como nacional, existen referencias clave que orientan las acciones de prevención, control y respuesta ante incidentes.

Una de las principales guías es la norma ISO/IEC 27001, que establece un sistema de gestión de seguridad de la información (SGSI), basado en la evaluación de riesgos y la implementación de controles específicos (ISO/IEC, 2013). Complementariamente, la ISO/IEC 27002 desarrolla buenas prácticas para la gestión de controles de seguridad, abarcando temas como políticas organizacionales, control de accesos, criptografía, seguridad física y continuidad del negocio.

También son de referencia el marco NIST Cybersecurity Framework (EE.UU.), orientado a identificar, proteger, detectar, responder y recuperar activos digitales, y el marco COSO “Committee of Sponsoring Organizations of the Treadway Commission” de control interno, que integra el componente tecnológico como parte de los riesgos operacionales.

En Argentina, la Ley 25.326 de Protección de los Datos Personales obliga a las empresas a implementar medidas de seguridad adecuadas para el tratamiento de datos sensibles. A su vez, la Ley 27.401 de Responsabilidad Penal de las Personas Jurídicas establece que las empresas pueden ser penalmente responsables por delitos informáticos si no demuestran haber adoptado medidas de prevención razonables.

Impacto en las organizaciones

La ciberseguridad ha dejado de ser una preocupación exclusivamente técnica para convertirse en un eje estratégico transversal en la gestión organizacional. Los incidentes cibernéticos, especialmente aquellos vinculados al robo o secuestro de información, tienen consecuencias que trascienden lo operativo y afectan las esferas económicas, legales, reputacionales y de continuidad del negocio.

Los ciberataques generan pérdidas económicas directas e indirectas. Entre los costos directos se destacan los gastos asociados a la interrupción de servicios, la recuperación de datos, la contratación de servicios forenses y legales, y (en los casos de ransomware) los pagos de rescate. En términos indirectos, pueden mencionarse la pérdida de

oportunidades de negocio, la disminución de productividad y los costos derivados de la implementación urgente de nuevas medidas de seguridad.

De acuerdo con el Informe sobre Costos de una Filtración de Datos de IBM Security (2021), el costo promedio de un incidente de seguridad superó los 4 millones de dólares, siendo más elevado en sectores como salud y servicios financieros.

Uno de los efectos más difíciles de revertir es el daño a la reputación institucional. La pérdida de información confidencial de clientes, empleados o proveedores suele derivar en una fuerte caída en la confianza de los públicos estratégicos, lo que puede afectar las relaciones comerciales, el valor de la marca e incluso provocar litigios judiciales. En un entorno cada vez más exigente con el resguardo de datos personales y corporativos, las empresas que no protegen adecuadamente su información se ven expuestas a un escrutinio social y legal cada vez mayor.

Un ejemplo ilustrativo de estas consecuencias ocurrió en 2021, cuando un importante laboratorio de análisis clínicos de Argentina sufrió un ataque de ransomware que comprometió gravemente su operación. Los atacantes lograron cifrar los archivos de sus sistemas internos, paralizando la entrega de resultados médicos y afectando la atención al paciente durante varios días. Además del impacto operativo inmediato, el incidente generó una crisis de confianza pública, especialmente por tratarse de información sensible vinculada a la salud de miles de personas.

Este caso motivó la intervención de la Agencia de Acceso a la Información Pública (AAIP), que inició una investigación por posible incumplimiento de la Ley 25.326. El laboratorio debió afrontar no solo los costos de recuperación y actualización tecnológica, sino también posibles sanciones legales por no haber demostrado fehacientemente la existencia de mecanismos de protección adecuados.

Este ataque también reflejó una problemática estructural en muchas organizaciones: la ausencia de políticas de continuidad del negocio, la falta de segmentación de redes internas y el uso deficiente de medidas como el cifrado de datos o doble factor de autenticación. Asimismo, evidenció el escaso entrenamiento de los usuarios ante amenazas como correos electrónicos maliciosos (método habitual de entrada para este tipo de malware).

En resumen, el impacto de los incidentes de ciberseguridad se manifiesta en múltiples dimensiones. En lo económico, los costos pueden incluir rescates pagados, inversiones en recuperación, pérdida de ingresos y sanciones. En lo legal, las organizaciones pueden enfrentar consecuencias derivadas del incumplimiento normativo, incluyendo responsabilidades penales bajo la Ley 27.401. En términos reputacionales, la pérdida de confianza por parte de clientes, proveedores y socios puede tener efectos a largo plazo, especialmente en un entorno cada vez más exigente con la gestión ética de la información.

Por estas razones, la ciberseguridad se ha convertido en un eje clave de la gestión empresarial moderna, y su abordaje ya no puede limitarse al área técnica, sino que debe involucrar activamente a todos los actores organizacionales, incluido el contador.

Abordaje empresarial

La ciberseguridad contemporánea enfrenta un entorno cada vez más volátil, incierto, complejo y ambiguo, caracterizado por el acrónimo VUCA (Volatility, Uncertainty, Complexity, Ambiguity) adoptado desde el ámbito militar y aplicado a la gestión estratégica de riesgos digitales. Las organizaciones deben actuar no solo de forma reactiva ante incidentes, sino con un enfoque proactivo y sistémico que contemple las múltiples dimensiones del riesgo cibernético.

Uno de los desafíos principales radica en la creciente complejidad de los entornos informáticos. La virtualización, la adopción de tecnologías en la nube, el trabajo remoto, el uso masivo de dispositivos móviles y la Internet de las Cosas (IoT) han ampliado significativamente la superficie de ataque. Cada nuevo punto de conexión representa un posible vector de intrusión, especialmente cuando las arquitecturas de red carecen de segmentación, monitoreo o control de acceso adecuado.

Un dispositivo IoT es cualquier objeto físico que puede conectarse a internet para recopilar y transmitir datos. Estos dispositivos, que pueden incluir desde electrodomésticos hasta sensores industriales, utilizan diversas tecnologías para comunicarse y permitir el monitoreo, control y análisis remotos. En muchos casos, son diseñados sin criterios de ciberseguridad desde el origen. Se han documentado vulnerabilidades críticas en cámaras de vigilancia, electrodomésticos inteligentes, cerraduras digitales y sensores industriales, lo cual expone a empresas e infraestructuras críticas a ataques o secuestros de dispositivos.

La falta de formación, la baja percepción del riesgo y la ausencia de protocolos de comportamiento seguro incrementan la probabilidad de incidentes. El personal no técnico, muchas veces, no distingue correos maliciosos ni comprende la sensibilidad de la información que maneja. La alta rotación laboral y la tercerización de servicios técnicos también dificultan la consolidación de una cultura de seguridad sostenida en el tiempo. Según estudios internacionales (PwC, SANS Institute), el 80% de los incidentes de ciberseguridad involucran phishing, y el 48% son originados por errores del usuario, lo que evidencia que el factor humano continúa siendo el eslabón más débil en la cadena de seguridad.

Bajo este marco, empresas como PwC realizan simulaciones de phishing, las cuales forman parte de los programas de concientización en ciberseguridad, buscando así reforzar la preparación del capital humano frente a amenazas reales. Una simulación de phishing consiste en el envío de correos electrónicos falsos pero verosímiles (simulando comunicaciones internas, bancos, proveedores, etc.) a empleados de una organización, sin advertencia previa. El objetivo es evaluar si los destinatarios hacen clic en enlaces sospechosos, ingresan credenciales o descargan archivos adjuntos, y luego utilizar los resultados como base para acciones correctivas y de formación. En caso de que el empleado efectivamente denuncie el mail como phishing, recibirá una notificación confirmando que el correo en cuestión pertenecía a una simulación y que dicho reporte fue realizado correctamente. Se adjunta en el anexo un caso de análisis.

El nuevo rol del contador estratégico

En un contexto marcado por la transformación digital, el contador ha dejado de ser un mero registrador de operaciones financieras para convertirse en un actor estratégico en la gestión organizacional. Esta evolución ha llevado al abandono de los registros contables físicos y la adopción de formatos digitales, lo que ha optimizado los procesos y permitido un análisis más eficiente de la información. Este nuevo enfoque implica ampliar su campo de acción hacia áreas como la gestión de riesgos, la auditoría de sistemas y el cumplimiento normativo, todas ellas atravesadas por la creciente necesidad de proteger los datos y garantizar la seguridad de la información. Organismos internacionales como IFAC (International Federation of Accountants) y FACPCE (Federación Argentina de Consejos Profesionales de Ciencias Económicas) promueven principios éticos que hoy se vinculan directamente con la ciberseguridad: confidencialidad, integridad y comportamiento profesional. Asimismo, se recomienda al profesional contable:

- Integrar el análisis de ciberseguridad en los procesos de control interno y auditoría.
- Promover la capacitación continua en temas digitales.
- Participar en la definición de políticas organizacionales sobre protección de datos y seguridad informática.

Estas prácticas no sólo fortalecen el ejercicio profesional, sino que contribuyen a una cultura de seguridad organizacional basada en la prevención, la responsabilidad compartida y la gestión informada del riesgo.

En materia de ciberseguridad, el contador estratégico se posiciona entonces como un actor clave en la prevención, detección y gestión de riesgos de información, desde una perspectiva ética, normativa y operativa. A continuación, se detallan los roles fundamentales que debe asumir:

1. Garante de la integridad de la información. El contador tiene la responsabilidad de asegurar que los datos financieros, tributarios y operativos no sean alterados, manipulados o accedidos sin autorización. Esto implica verificar la existencia de controles internos robustos que protejan la integridad y la trazabilidad de los registros contables. A modo de ejemplo, puede pensarse el detectar inconsistencias que podrían surgir de accesos no autorizados o manipulación fraudulenta de datos por parte de usuarios internos o externos.

2. Participación en auditorías digitales y de sistemas. Debe colaborar activamente en la auditoría de sistemas de información y procesos digitales, evaluando los riesgos asociados al uso de tecnologías, accesos indebidos, vulnerabilidades y brechas de seguridad.

3. Evaluación del cumplimiento normativo. El contador es el profesional indicado para verificar el cumplimiento de normativas tanto contables como de protección de datos personales (por ejemplo, Ley 25.326) y responsabilidad penal empresarial (Ley 27.401). Debe asegurarse de que la empresa adopte políticas claras sobre confidencialidad, uso de la información y protección de activos digitales.

4. Articulador interdisciplinario. El contador cumple un rol de puente entre áreas técnicas y de gestión, facilitando la comunicación entre el área de sistemas, los equipos legales y los directivos. Su conocimiento transversal del

negocio le permite contextualizar los riesgos tecnológicos dentro de los procesos financieros y operativos de la organización.

5. Diseñador y evaluador de controles internos. Debe participar en el diseño y la evaluación de controles preventivos, como la segregación de funciones, límites de acceso, cifrado de datos contables, respaldos automáticos y autenticación de usuarios. Estos controles forman parte esencial de los sistemas de gestión del riesgo, y su ausencia puede derivar en fraudes o incidentes de ciberseguridad.

6. Promotor de la cultura ética y la formación continua. Finalmente, el contador debe actuar como promotor de la ética profesional en contextos digitales, impulsando la formación continua en temas como confidencialidad, protección de la información, uso seguro de sistemas y cumplimiento normativo.

Este nuevo perfil, por lo tanto, requiere del contador el desarrollo de competencias transversales, entre ellas:

- Conocimiento básico de tecnologías de la información y ciberseguridad, incluyendo marcos como ISO 27001, NIST y COSO.
- Capacidad de análisis de riesgos asociados a procesos digitales.
- Actualización normativa permanente, en materia contable, fiscal y de protección de datos.
- Habilidades de comunicación y trabajo interdisciplinario, para interactuar con áreas legales, de sistemas, auditoría interna y dirección.

En este sentido, el contador se posiciona como un actor clave entre lo contable, lo legal y lo tecnológico, ayudando a traducir los requerimientos normativos y de control interno en prácticas concretas dentro de los sistemas de gestión. Su visión integral del negocio lo convierte en un actor esencial para garantizar la integridad y confiabilidad de la información, en un entorno cada vez más expuesto a riesgos digitales.

Este nuevo enfoque profesional, basado en la ética, la prevención y la gestión del conocimiento, no solo fortalece la función contable, sino que la proyecta como una pieza fundamental en la sostenibilidad informativa y económica de las organizaciones.

Conclusión

La creciente digitalización de los procesos organizacionales ha convertido a la ciberseguridad en una prioridad estratégica para las empresas, sin importar su tamaño o sector. En este escenario, los datos se constituyen como uno de los activos más valiosos, y su protección resulta indispensable para garantizar la continuidad operativa, el cumplimiento legal y la confianza de los distintos públicos interesados.

Lejos de ser un tema exclusivo del área tecnológica, la ciberseguridad exige un enfoque transversal, en el cual el profesional contable ocupa un lugar destacado. Su conocimiento de los procesos, su rol en el control interno, su capacidad de análisis y su compromiso ético lo posicionan como un aliado clave en la gestión de riesgos informáticos.

Este nuevo contexto demanda al contador una actualización permanente, tanto en términos normativos como tecnológicos, y una disposición activa para colaborar con otras áreas organizacionales. Adoptar buenas prácticas, participar en auditorías de sistemas, contribuir al cumplimiento de marcos normativos y promover una cultura de seguridad son hoy parte esencial de su función estratégica.

La ciberseguridad, entendida como un esfuerzo colectivo y sostenido, requiere de profesionales con visión integral y compromiso con la transparencia. En ese camino, el contador del siglo XXI tiene mucho para aportar.

Resumiendo lo anterior, podemos agrupar la información en la siguiente línea de tiempo:

Período/Etapa	Tecnología	Ciberseguridad/Riesgos	Impacto Organizacional	Rol del Contador
Época Predigital y Transición (Antes de los 2000s)	Registros contables principalmente físicos y manuales. Digitalización incipiente.	Preocupaciones limitadas a la seguridad física de documentos y acceso a información en papel.	Gestión de riesgos centrada en el ámbito físico.	Tradicionalmente vinculado al registro de operaciones, control financiero y elaboración de estados contables impresos.
Era de la Dependencia Digital y Primeros Desafíos (Inicios 2000s - Aprox. 2010)	Abandono gradual de registros físicos y adopción masiva de formatos digitales. Creciente dependencia de sistemas informáticos.	Ciberseguridad percibida como asunto técnico de TI. Emergencia de amenazas como malware y virus.	Empresas experimentan pérdidas económicas iniciales por ataques informáticos.	Enfoque tradicional, pero la integridad y confidencialidad de la información digital comienza a ser un desafío incipiente.
Madurez del Riesgo y Concienciación Transversal (Aprox. 2010 - Mediados 2020s)	Expansión de trabajo remoto, tecnologías en la nube, uso intensivo de dispositivos móviles y la Internet de las Cosas (IoT) amplían la "superficie de ataque".	Amenazas más sofisticadas y frecuentes: phishing, ransomware, fuga/pérdida de datos, suplantación de identidad. Factor humano reconocido como "eslabón más débil". Marcos legales/normativos (ISO/IEC 27001, NIST, COSO, Leyes argentinas 25.326 y 27.401).	Ciberseguridad se convierte en "eje estratégico transversal". Incidentes generan pérdidas económicas (costo promedio >$4M), consecuencias legales y daño reputacional significativo (ej. Caso laboratorio clínico argentino en 2021).	Comienza a ser reconocido como actor clave en la gestión de riesgos digitales. Organismos (IFAC, FACPCE) promueven principios éticos ligados a ciberseguridad. Se le recomienda integrar análisis en control interno y auditoría.
El Contador Estratégico y la Ciberseguridad como Prioridad (Desde Mediados 2020s en adelante - Siglo XXI)	Entorno VUCA en ciberseguridad. Enfoque proactivo y sistémico. Implementación de programas de concientización (simulaciones de phishing).	La ciberseguridad es una prioridad estratégica global. Datos son un activo valioso, su protección es indispensable.	Ciberseguridad es un "esfuerzo colectivo y sostenido". Empresas requieren visión integral y compromiso con la transparencia.	Se consolida como "actor estratégico" y "transversal". Roles fundamentales: garante de integridad, participación en auditorías digitales, evaluador de cumplimiento normativo, articulador interdisciplinario, diseñador de controles, promotor de cultura ética y formación continua. Necesidad de nuevas competencias (TI, ciberseguridad, análisis de riesgos, actualización normativa, comunicación).

Anexo 1

Simulación Phishing

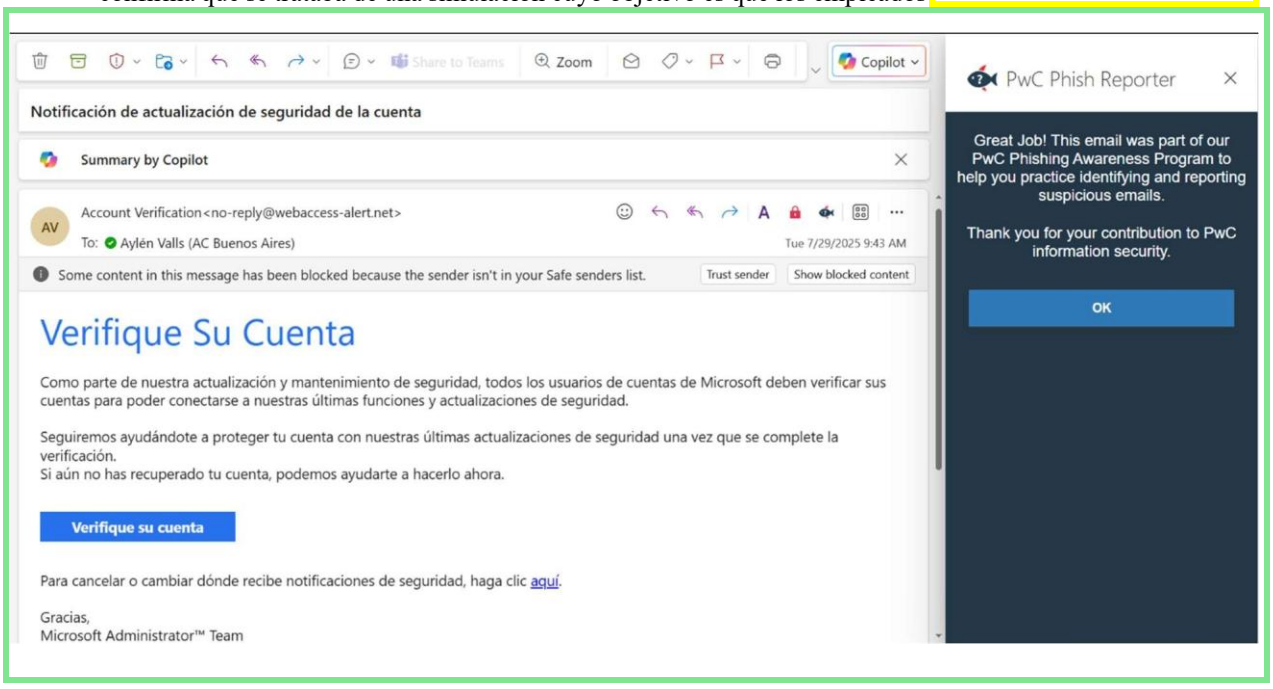
Para una mayor comprensión, se han hecho recuadros de colores al caso de estudio. Véase el cuadro:

a. Rosa. Corresponde a la casilla que envía el mail en cuestión. Debe notarse que, si bien el cuerpo del mail "corresponde" a una notificación de Microsoft Teams, la dirección de correo no pertenece a dicha organización.

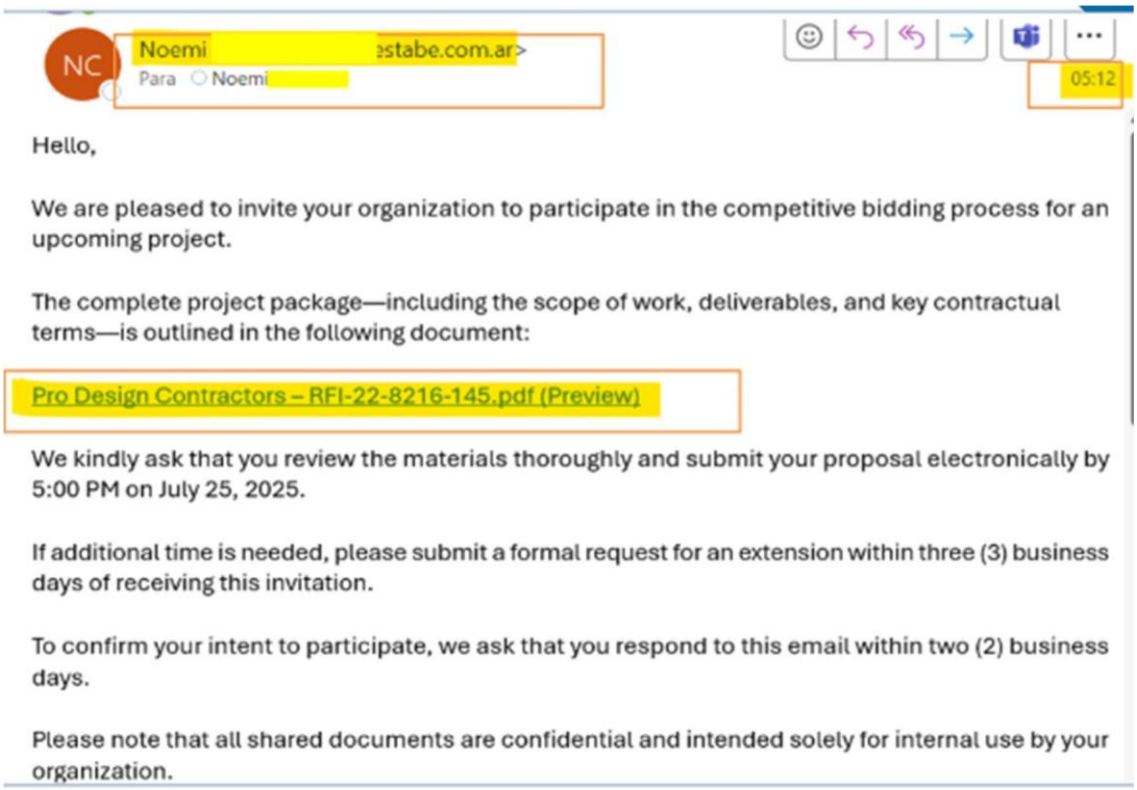
b. Verde. Es el cuerpo del mail, el mismo se encuentra bien redactado y sin faltas de ortografía. Asimismo, incluye links que, de ser realmente phishing, tienen por objeto que una vez que el usuario haga click en ellos, lo redireccione a una página diseñada para obtener información confidencial.

c. Rojo. Botón para alertar de un posible phishing.

d. Amarillo. Al denunciar el mail como phishing correctamente, la empresa confirma que se trataba de una simulación cuyo objetivo es que los empleados practiquen el identificar y reportar mails sospechosos.



Anexo 2



Para una mayor comprensión, se han resaltado los aspectos a considerar en caso de estudio. Véase el cuadro:

a. La identificación del remitente se basa en un nombre real, sin embargo la dirección de correo electrónica de la que procede es la inadecuada, no corresponde a la empresa.
b. La hora del envío de la comunicación no es un horario laboral que se maneje en la empresa o que dicha persona use para compartir comunicaciones.
c. Se relaciona un vínculo con un archivo tipo .pdf que normalmente no se enviaría dado que se manejan bases de datos compartidas a las que tiene acceso el equipo de trabajo.

Anexo 3

Caso Clorox Agosto 2023

En agosto de 2023, Clorox detectó actividad no autorizada en sus sistemas de TI, lo que derivó en interrupciones operativas prolongadas y graves problemas en la producción y distribución. La compañía reportó a la SEC una caída proyectada del 23 % al 28 % en las ventas netas del primer trimestre fiscal, un impacto en sus ganancias por acción de entre 0,35 y 0,75 dólares, retrasos significativos en el procesamiento de pedidos y escasez de productos como Pine-Sol, Brita, Glad y Burt's Bees. El ataque obligó a implementar procesos manuales y afectó gravemente su infraestructura tecnológica.

Las pérdidas estimadas ascendieron a unos 356 millones de dólares, evidenciando el alto costo financiero y operativo de un ciberataque. El incidente mostró cómo tácticas como la ingeniería social y vulnerabilidades en áreas críticas como las mesas de ayuda de TI pueden escalar rápidamente a crisis corporativas de gran magnitud. El caso refuerza la necesidad de contar con verificaciones de identidad más robustas, planes de ciberresiliencia y estrategias preventivas para proteger la continuidad operativa.

Clorox presentó una demanda por 380 millones de dólares contra Cognizant, su proveedor de servicios de mesa de ayuda (help desk), luego de un ciberataque ocurrido en agosto de 2023. Según la denuncia, el grupo de hackers conocido como Scattered Spider logró infiltrarse mediante ingeniería social, accediendo a sistemas críticos debido a que Cognizant entregó credenciales sin verificar la identidad del solicitante, lo que interrumpió la producción y el envío de productos durante meses.

El ataque no resultó de una vulnerabilidad tecnológica, sino de errores humanos graves: en llamadas telefónicas, los estafadores se hicieron pasar por empleados, solicitaron restablecimientos de contraseña y los recibieron sin confirmación alguna, incluso habilitando acceso sin autenticación multifactor. Clorox sostiene que Cognizant no solo violó los protocolos internos y entregó las claves, sino que también falló en la respuesta al incidente, retrasando la recuperación de sus sistemas.

Cognizant ha rechazado las acusaciones, afirmando que su rol estaba limitado a brindar soporte técnico dentro del alcance contratado y que no era responsable de la seguridad general de los sistemas de Clorox. No obstante, expertos en seguridad han señalado que la facilidad con la que se entregaron las credenciales sugiere negligencia y no un sofisticado ataque.

Anexo 4

Casos de estudio respecto de las regulaciones y las certificaciones Casos de aplicación de la ley nacional:

Ley 25.326: Protección de los datos personales: La resolución de la Agencia de Acceso a la Información Pública (AAIP) estableció que Swiss Medical S.A. incumplió con el deber de confidencialidad y el principio de consentimiento que establece la Ley al entregar a un empleador el historial clínico de un paciente en el año 2024 sin su consentimiento.

Ley 26.388 Ciberdelitos: Caso acceso ilegítimo por un ciberataque a una base de datos de información pública y el daño informático al Registro Nacional de las Personas (RENAPER) entidad del Estado. y Caso Rapi en la que la AAIP

interpuso una multa de 15Millones de pesos ARS, por no haber adoptado las medidas técnicas y organizativas para garantizar la seguridad y confidencialidad de los datos.

Ley 27.401: Responsabilidad Penal de las Personas Jurídicas: En 2020, la Casa Matriz de la empresa de seguridad sueca Securitas, -tras una auditoría interna-, descubrió que su filial en Argentina había pagado sobornos millonarios a funcionarios de diversos organismos públicos para obtener contratos y otros beneficios ilícitos. Las maniobras incluían el uso de proveedores falsos y sobrefacturación para generar los fondos destinados a los sobornos a funcionarios de organismos como el RENAPER, AYSA y
SENASA, entre otros. Se puede observar en el siguiente link https://www.youtube.com/watch?v=pd7mjVSL4tk información relevante del proceso, debido a que el proceso surte por la autodenuncia de la empresa sueca ante el organismo argentino.

Casos fallidos en el cumplimiento de las certificaciones internacionales:

1. ISO/IEC 27001 y 27002: En 2013 y 2014, Yahoo! sufrió filtraciones de datos, afectando a más de 3 mil millones de cuentas. Los atacantes robaron nombres, direcciones de correo electrónico, números de teléfono, fechas de nacimiento, contraseñas hash y preguntas de seguridad.

2. NIST: Fallo del control sobre las cinco funciones del marco NIST (Identificar, proteger, detectar, responder y recuperar) en la empresa Equifax agencia de crédito en 2017. El ataque se produjo a través de una vulnerabilidad crítica en el software Apache Struts.

3. COSO: Falla en el ambiente de control y análisis de riesgos en la empresa Wells Fargo & Company de California que detonó entre 2011 y 2016, donde empleados abrieron más de 2 millones de cuentas de clientes no autorizadas sin su consentimiento. El fraude se produjo debido a una presión desmedida por alcanzar metas de venta que se reflejaban en los sistemas de incentivos de la empresa.

Referencias

International Organization for Standardization. (2013). ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements. https://www.iso.org/isoiec-27001-information-security.html

International Organization for Standardization. (2013). ISO/IEC 27002:2013 – Code of practice for information security controls. https://www.iso.org/standard/54533.html

Instituto Nacional de Estándares y Tecnología (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://www.nist.gov/cyberframework

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.República Argentina. (2000). Ley 25.326 – Protección de los Datos Personales. Boletín Oficial de la República Argentina.

República Argentina. (2017). Ley 27.401 – Responsabilidad Penal de las Personas Jurídicas. Boletín Oficial de la República Argentina.

IFAC. (2020). The Role of Professional Accountants in Data Governance. https://www.ifac.org/knowledgegateway

FACPCE. (2021). Ética profesional y desafíos en entornos digitales. Documento técnico interno.

Magazcitum. (2017, abril). Concientización en seguridad de la información. https://magazcitum.com

Documento interno. (2021). Introducción a la seguridad de la información. Archivo compartido por el usuario.

The Institute of Internal Auditors. (2025). Global Summary: Risk in Focus 2025 – Hot Topics for internal auditors. https://www.theiia.org/RiskinFocus

International Organization for Standardization. (2013). Disponible en: https://www.normaiso27001.es/#h1

Instituto Nacional de Estándares y Tecnología (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity. Disponible en: https://www.nist.gov/cyberframework

República Argentina. (2000). Ley 25.326 – Protección de los Datos Personales. Boletín Oficial de la República Argentina. Disponible en: https://www.argentina.gob.ar/normativa/nacional/ley-2532664790/normas-modifican

República Argentina. (2017). Ley 27.401 – Responsabilidad Penal de las Personas Jurídicas. Boletín Oficial de la República Argentina. Disponible en: https://www.boletinoficial.gob.ar/detalleAviso/primera/175501/20171201?busqueda=1

IFAC. (2020). The Role of Professional Accountants in Data Governance. Disponible en: https://www.ifac.org/knowledge-gateway

República Argentina. (2024). Fuga de datos en el RENAPER Disponible en: https://revistainnovacion.com/nota/12307/fuga_de_datos_en_el_renaper/

República Argentina. (2024). Fallo divulgación de historia clínica. Disponible en: https://aldiaargentina.microjuris.com/2024/06/10/fallos-divulgacion-de-historia-clinica-una-prepaga-debeser-multada-por-haber-divulgado-la-historia-clinica-de-una-paciente-a-su-empleador/

Polanco, M. (2025). Nadie sabe los activos que tiene hasta que lo “hackean” (gestión de activos para la ciberseguridad). Magazcitum, 16(1), 14–15.

Hale, C. (2025, July 24). Clorox seeks $380M from Cognizant over help desk failures in cyberattack. Cybersecurity Dive. https://www.cybersecuritydive.com/news/clorox-380-million-suit-cognizantcyberattack/753837/

ThriveDX. (2023, noviembre 10). The Clorox Company's 2023 cyberattack: Major fallout, system disruptions & product shortages. ThriveDX. https://thrivedx.com/resources/article/clorox-companys-2023cyberattack-fallout

Recursos adicionales:

Etica en el sector público: https://www.rite.gob.ar/

Ciberseguridad: https://capacitacion.inap.gob.ar/

En la página del Gobierno de la ciudad el Grupo de Trabajo "Concientización y Educación", perteneciente al Comité Nacional de Ciberseguridad-informe 2023
https://www.argentina.gob.ar/sites/default/files/2023/11/gt_educacion_y_concientizacion_nov2023.pdf

Marco de ciberseguridad - NIST: https://www.nist.gov/cyberframework

COSO y las 3LD: https://iaia.org.ar/2016/10/25/marco-referencia-coso-control-interno-modelo-tres-lineasdefensa-caso-la-eficiencia-versus-la-proteccion-la-industria-servicios-financieros/

Recursos sobre Ciberseguridad del AIC: https://contadores-aic.org/fortaleciendo-la-resiliencia-digital-estrategias-de-ciberseguridad-para-los-contadores-de-las-americas/

Recurso didáctico formativo Google Interland: https://beinternetawesome.withgoogle.com/es419_all/interland

Ciber para niños y adultos https://cyberscouts.osi.es/