VOL. 2, NRO. 1
JUNIO - NOVIEMBRE 2022

ISSN 2718-8647

AUDIT.AR
REVISTA DE AUDITORÍA

ENSAYO

# AUDITORÍA EXTERNA Y CIBERSEGURIDAD

# EXTERNAL AUDIT AND CYBERSECURITY

**Martín Ghirardotti**
**Profesor titular de la Diplomatura en Governance, Compliance, Control & Assurance - Universidad de San Andrés. Argentina.**
mghirardotti@llyasoc.com

**Juan Ignacio Renna**
**Facultad de Ciencias Económicas. Universidad Nacional de Cuyo. Argentina.**
jrenna@llyasoc.com

## RESUMEN

Este ensayo tiene como objetivo sentar una discusión argumentativa sobre un tema de actualidad que involucra tanto a empresas como organismos reguladores y auditores externos. De allí, que estos últimos comiencen a adaptar la planificación y ejecución de alguno de sus trabajos. Asimismo, se analizará el tema desde un contexto novedoso y cambiante en Latinoamérica, sin perder de vista el impacto en organismos reguladores y firmas de auditores en Estados Unidos y Europa. Finalmente, este ensayo propondrá una visión a futuro respecto del surgimiento de nuevas necesidades en materia de ciberseguridad, por parte de las empresas, y herramientas con las cuales podría contar el auditor externo para desarrollar su labor en auditorías.

## ABSTRACT

This essay aims to set up an argumentative debate on a current issue, which involves companies, regulatory bodies and external auditors. Thus, the latter are beginning to adapt the planning and performance of some of their work. Moreover, the matter will be analysed from a novel and changing context in Latin America but taking into consideration the impact on regulatory bodies and auditing firms in the United States. and Europe.

Finally, this essay will provide future prospects about the emergence of new companies´needs regarding cybersecurity and tools which the external auditors could rely on when carrying out their audits.

## PALABRAS CLAVE

auditoría, ciberseguridad, riesgos

## KEYWORDS

audit, cybersecurity, risks

**AUDITORÍA EXTERNA Y CIBERSEGURIDAD**

**AUTORES:**
Martín Ghirardotti -
Juan Ignacio Renna

**RECIBIDO:**
12 de marzo, 2022

**APROBADO:**
3 de junio, 2022

**AUDITAR**
**PRIMERA REVISTA ARGENTINA**
**EXCLUSIVA SOBRE AUDITORÍA**

**DOI:** https://doi.org/10.24215/27188647e014
**CÓDIGO JEL:** M42
**ISSN:** 2718-8647
http://revistas.unlp.edu.ar/auditar

**ENTIDAD EDITORA:**
Instituto de Investigaciones y Estudios Contables, Facultad de Ciencias Económicas, Universidad Nacional de La Plata

## INTRODUCCIÓN

El desarrollo de las empresas no es ajeno a la globalización y el avance de las tecnologías. Desde hace años, vivimos en una era de transformación digital que, definitivamente, ha llegado para quedarse y continuará su vertiginosa evolución, inclusive, al punto de dejar relegados a quienes no tienen la posibilidad de reinventarse y/o adaptarse a ella. En este sentido, la aparición del virus SARS-CoV-2, las consecuentes restricciones de circulación y las nuevas condiciones de trabajo remoto aceleraron el proceso de inclusión de tecnologías digitales en las empresas. Esto, generó una dependencia tecnológica cada vez mayor, y con ella, un incremento de los riesgos asociados a la ciberseguridad que ha dado lugar a incidentes cibernéticos.

La tecnología se ha transformado en un imperativo estratégico, tanto para empresas como para auditores y organismos reguladores de todo el mundo. El tiempo es considerado un recurso cada vez más valioso, y la tecnología y los esfuerzos de las personas apuntan con frecuencia a su optimización. Las organizaciones para la gestión y el manejo de la información, los auditores que desarrollan su trabajo y aplican procedimientos con el fin de tener un grado de seguridad razonable sobre la información objeto de auditoría, y los organismos de control en el mundo deben acompañar el desarrollo tecnológico, ya sea para optimizar sus procesos como para adecuarse a tecnologías utilizadas por las entidades que regulan. En Latinoamérica y particularmente en Argentina, muchos organismos reguladores han tendido a automatizar procesos por medio de la digitalización de la información y de usuarios virtuales, viéndose obligados a buscar alternativas a los trámites presenciales.

Si bien esto implica un importante avance para la profesión, las amenazas a la seguridad cibernética derivadas de la conectividad y el desarrollo tecnológico de vanguardia no deben ser soslayadas. La gravedad de las amenazas y las posibles consecuencias para las empresas, auditores, reguladores, inversores y la economía en general, van en aumento. A medida que los mercados, sus participantes y proveedores confían en la tecnología –incluso en conexiones y sistemas digitales– la gestión de riesgos de ciberseguridad se ha vuelto esencial. En un contexto donde los agresores cibernéticos se vuelven más peligrosos y sofisticados -en muchos casos incentivados por recursos sustanciales y el respaldo de actores de estados nacionales- la triada empresa-auditor-organismo de control se enfoca en el modo en que los riesgos deben ser analizados por cada organización, en el marco de sus obligaciones internas. Ahora bien, ¿qué se entiende por ciberseguridad? Según el Centro de Recursos de Seguridad Informática (CSRC por sus siglas en inglés) del Instituto Nacional de Estándares y Tecnología del Departamento de Comercio de Estados Unidos (NIST por sus siglas en inglés) un ciberataque es

> un ataque, a través del ciberespacio, dirigido al uso del ciberespacio por parte de una empresa, con el propósito de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno o infraestructura informática, o destruir la integridad de los datos o robar información controlada. (CSRC, s.f, Cyber Attack)

Por su parte, la Asociación de Auditoría y Control en Sistemas de Información (ISACA por sus siglas en inglés) entiende por ciberseguridad la "protección de los activos de información al abordar las amenazas a la información procesada, almacenada y transportada por los sistemas de información interconectados."[1] (ISACA, s.f, Cybersecurity)

Definida en forma sencilla, la ciberseguridad comprende las prácticas para defender de un ataque malicioso a los dispositivos, sistemas, datos y redes conectados en un ciberespacio. El Instituto de Contadores Públicos Certificados de Estados Unidos (AICPA por sus siglas en inglés) explica la diferencia entre seguridad cibernética y seguridad de la información, y define aquella como aquellos

> procesos y controles implementados por una entidad para gestionar los riesgos de ciberseguridad. Debido a que los procesos y controles que abordan los riesgos de seguridad cibernética también abordan la gran mayoría de los otros riesgos de seguridad de la información de la entidad, los términos seguridad cibernética y seguridad de la información a menudo se usan indistintamente. La principal diferencia

[1] La traducción es nuestra

> entre la seguridad de la información y la ciberseguridad es que la seguridad de la información también aborda los riesgos que surgen de los sistemas informáticos que están físicamente aislados de otros sistemas electrónicos y la protección de la información almacenada en un formato que no es accesible a través de medios electrónicos (como papel impreso almacenado en archivadores)[2]. (AICPA, s.f, SOC for Cybersecurity: Information for CPAs)

Las tecnologías emergentes y el análisis de datos están revolucionando la forma en que se prepara y presenta la información financiera, cómo se realizan las auditorías y, en última instancia, cómo diagraman sus controles los organismos reguladores. Las empresas realizan cada vez más tareas utilizando algoritmos y automatización robótica de procesos, al tiempo que aumentan el uso de análisis avanzados e inteligencia artificial en sus informes. Los auditores, estamos explorando nuevos enfoques de tecnología y análisis de datos para obtener información confiable y suficiente que nos permita realizar nuestros trabajos. En la actualidad, para citar un ejemplo, acudimos a medios digitales como videollamadas o drones para realizar observaciones de inventario. Asimismo, prevemos que el análisis de datos del futuro podría reemplazar las técnicas de muestreo actuales utilizadas para el análisis de todas las transacciones y cuentas.

La tecnología nos promete un combo perfecto: potenciar eficiencia con una mayor eficacia, lo que debería significar una mejor calidad de auditoría, ya que la reducción de procedimientos sustantivos manuales generaría tiempos disponibles para agudizar nuestro escepticismo profesional y con ello, la capacidad para identificar indicadores de error o fraude. No obstante esta oferta tentadora, las tecnologías emergentes presentan riesgos reales, y su impacto en los estados financieros no suele ser bajo, lo que implica un mayor riesgo para el auditor externo a la hora de realizar el proceso de auditoría. Entre los más importante se destacan:

> Errores de codificación: comprende un error durante el proceso de codificación de datos. Dependiendo de la naturaleza, los resultados del error de codificación son variables. Los errores de codificación ocurren por una amplia variedad de razones con todo tipo de tecnología, aunque existen varias salvaguardas diseñadas para minimizar o prevenir tales errores. Algunos, ocurren durante el desarrollo o cuando se realizan cambios después de la implementación; otros errores pueden permanecer latentes durante largos períodos.
>
> Sesgo no intencionado o algorítmico: este sesgo ocurre cuando los errores sistemáticos y repetibles en el software o los sistemas informáticos provocan resultados inexactos que privilegian, arbitrariamente, un resultado sobre otro. El sesgo puede surgir del diseño de un algoritmo en sí o a través de usos no previstos.
>
> Accesos no autorizados: este riesgo está dado por la posibilidad de que usuarios no autorizados o, peor aún, personas ajenas a la organización accedan a datos o información confidencial. Lo que potencia esta amenaza es la alta conectividad tecnológica, de redes y sistemas de comunicación. Esta interconexión se produce a través de sistemas de telecomunicaciones y, principalmente, a través de internet. La amenaza cibernética apunta principalmente a este último riesgo e incluye la pérdida de información privada y confidencial, la manipulación y destrucción de datos, sistemas y redes, e incluso, el daño o sustracción de activos físicos, así como los costos reputacionales que esto puede acarrear. A medida que integramos la tecnología en todo lo que hacemos (infraestructuras críticas, redes de comunicación y dispositivos de consumo), las ciber-amenazas suponen un riesgo cada vez mayor y particularmente, ese es el camino hacia donde se dirigen las empresas en cuanto al manejo de su información.

## EL ROL DEL AUDITOR EXTERNO EN RELACIÓN CON AMENAZAS DE SEGURIDAD CIBERNÉTICA

Actualmente, en nuestra tarea como auditores de estados financieros desempeñamos un papel limitado respecto de la seguridad cibernética. Normalmente, no evaluamos en profundidad el riesgo de seguridad cibernética de la empresa ni el diseño y la eficacia de los controles operativos y otros controles no financieros para mitigar ese riesgo. Por el contrario, sí es habitual hacer foco en la tecnología de la información

[2] La traducción es nuestra

que utiliza la empresa auditada para preparar sus estados financieros. El auditor también suele centrarse en los procesos automatizados, empleados por la dirección de la entidad que prepara la información financiera, sobre los que no es posible aplicar procedimientos sustantivos, evaluando en tal caso, si los controles asociados a tales procesos mitigan riesgos de errores materiales sobre los estados financieros.

En casos poco frecuentes, cuando el auditor externo se encuentra con situaciones en donde se evidencian temas de seguridad cibernética, debe enfocarse en dos puntos principales, aunque no excluyentes:

· Incidentes relacionados con la seguridad cibernética, revelados en los estados financieros de la entidad: en este caso, el auditor evalúa si dichos estados tomados en su conjunto están presentados fielmente de acuerdo con los principios de contabilidad generalmente aceptados que sean de aplicación, en todos los aspectos significativos. Por ejemplo, si una empresa registra un pasivo contingente significativo, a causa de un incidente relacionado con ciberseguridad, entonces el auditor evaluara la idoneidad de ese pasivo, su correcta medición, como también si la revelación sobre este tema en las notas a dichos estados financieros son adecuadas o no.

· Cuando la situación relacionada con la seguridad cibernética no está contenida en los estados financieros en sí, sino que se ha accedido a la información por otros medios o se encuentra en otra información, el papel es incluso más limitado. en este caso, el auditor debería solicitar dicha información y considerar si existe alguna incongruencia material con la información que contienen los estados financieros tomados en su conjunto, o con el conocimiento adquirido durante el desarrollo del trabajo (NIA 720, Revisada 2020, párr. 11).

Los auditores, deberíamos considerar la ciberseguridad como parte nuestra evaluación de riesgos de auditoría, salvo en casos donde una organización funcione completamente con procesos manuales, sin usar tecnología o internet, En la actualidad, pocas empresas se encuentran en esta situación o carecen de riesgos de seguridad cibernética, en particular, las empresas públicas. Como en muchos casos, quienes desarrollamos esta tarea en Latinoamérica debemos mirar al mundo y direccionar nuestro camino. En ese sentido, algunas firmas de auditores en Norteamérica o Europa se están interiorizando en temas de ciberseguridad y la consideran al momento de evaluar el riesgo de incorrecciones materiales en los estados financieros, sobre todo en empresas públicas. El AICPA por ejemplo, publicó una guía que proporciona algunos recursos para colaborar con profesionales y firmas de auditoría para evaluar riesgos o asesorar a empresas. Esta situación se ha potenciado, dado que en los últimos años los organismos de control de entidades públicas han iniciado sumarios o acciones en materia de ciberseguridad. Por ejemplo, hace un tiempo la comisión de bolsa y valores de Estados Unidos Security Exchange Commission (SEC por sus siglas en inglés) inició una acción judicial resuelta contra la empresa antes conocida como Yahoo! Inc. por engañar a los inversores al no revelar una filtración de información muy importante. El sucesor de Yahoo!, Altaba, pagó una multa de 35 millones de dólares. Esta, fue una de las primeras acciones de la SEC contra una empresa por violación de divulgación de seguridad cibernética (SEC, Accounting and Auditing Enforcement Release nº3937, 2018). Otro ejemplo, es el caso de SolarWinds y la filtración de datos conocida mundialmente hacia fines de 2020. Esta empresa de software cuenta con una amplia y prestigiosa cartera de clientes y se estima que 18.000 de ellos descargaron una versión pirateada de su software, que los ciberdelincuentes manipularon para un acceso futuro. Sin embargo, solo una pequeña cantidad identificó la intromisión, lo que sugiere que los atacantes infectaron muchas más empresas de las que finalmente victimizaron. Además, se cree según publicaciones de la Agencia de noticias británica Reuters, que en este incidente estuvieron involucrados organismos de inteligencia rusos. Desde comienzos del año 2021, alrededor de 24 empresas han sido identificadas públicamente como afectadas, entre ellas Microsoft Corp., Cisco Systems, FireEye Inc. e Intel Corp. La SEC les pidió que entreguen registros de cualquier otra violación de datos o ciberataque, desde octubre de 2019 en adelante, en aquellos casos donde las empresas afectadas descargaron una actualización del software de administración de red de SolarWinds Corp con errores (Reuters, 2021).

Por último, podemos mencionar lo sucedido con Mercado Libre, que recientemente fue víctima de un acceso no autorizado que afectó a más de 300.000 usuarios. Si bien la compañía informó que los pro-

tocolos de seguridad se habían activado y que ningún sistema de infraestructura se había comprometido, esta situación, en muy poco tiempo, trajo consigo un fuerte impacto en la reputación de la empresa y en el precio de sus acciones. Asimismo, la empresa tuvo que informar sobre el incidente a la SEC, de acuerdo con lo dispuesto en su reglamentación; este organismo se encuentra estudiando el caso.

Estemos o no ante un incidente cibernético, durante el proceso de planificación los auditores deberíamos realizar una evaluación de riesgos tal que considere el diseño de los sistemas y su exposición a cualquier riesgo de seguridad cibernética que pueda tener un efecto material en los estados financieros de la empresa, y en tal caso, diseñar y ejecutar procedimientos para abordar dichos riesgos. Para ello, debemos obtener un entendimiento multidireccional de la empresa sujeto de auditoría y el ambiente de control en el cual opera (NIA 400). Esta comprensión, incluye los sistemas de tecnología de información relevantes para la información financiera, junto con cualquier subsistema relacionado. Asimismo, implica comprender los posibles puntos y controles de acceso a los sistemas. Los siguientes ítems podrían resultar una guía útil al momento de la evaluación de riesgos de la entidad:

- Aspectos del negocio y operaciones particulares que dan lugar a riesgos de ciberseguridad (industria en la que opera, sistemas y canales conectados a internet, etc.).
- El modo en que la entidad define el riesgo de ciberseguridad para su negocio.
- La entidad tiene un inventario (o no) de sus activos de información.
- El modo en que la entidad diseña su red y sus interfaces de sistemas.
- Alguno de los riesgos de ciberseguridad afecta al sistema de control interno global diseñado.
- Actitud tomada por la entidad respecto de la ciberseguridad como resultado de su evaluación de riesgos.
- Programa de ciberseguridad con estándares conocidos (implementación de normas ISO 27001) monitoreado por la dirección.
- Evaluación periódica (o no) del cumplimiento de políticas de ciberseguridad.
- Si han ocurrido (o no) incidentes de ciberseguridad en el pasado y su impacto.
- Evaluar la existencia de informes de terceros expertos e independientes respecto al seguimiento de mejores prácticas en ciberseguridad.

A continuación, se expone un cuadro con algunas de las ciberamenazas más comunes y su clasificación, según el impacto en el nivel de riesgos:

Tabla 1

**CRITERIOS DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES**

| NIVEL | AMENAZAS SUBYACENTES MÁS | VECTOR DE ATAQUE | CARACTERÍSTICAS POTENCIALES DEL |
|---|---|---|---|
| **CRÍTICO** | Ciberespionaje | Campañas de malware, compromiso de sistemas de control industrial, incidentes especiales. | - Capacidad para filtrar información muy valiosa, en cantidad y en poco tiempo.<br>- Capacidad para tomar el control de los sistemas sensibles, en cantidad y en poco tiempo. |
| **MUY ALTO** | - Interrupción de los Servicios IT. Exfiltración de datos. | - Códigos dañinos confirmados de Alto Impacto (RAT, troyanos enviando datos, rootkit, etcétera).<br>- Ataques externos con éxito. | - Capacidad para filtrar información valiosa, en cantidad apreciable.<br>- Capacidad para tomar el control de los sistemas sensibles considerable. |
| **ALTO** | - Toma de control de los sistemas. - Robo y publicación o venta de información sustraída. - Ciberdelito. - Suplantación. | - Códigos dañinos medio impacto (virus, gusanos, troyanos).<br>- Ataques externos compromiso de servicios no esenciales.<br>- Accesos no autorizados.<br>- Spear phising/pharming. | - Capacidad para filtrar información valiosa.<br>- Capacidad para tomar el control de ciertos sistemas. |
| **MEDIO** | - Logro o incremento de capacidades ofensivas.<br>- Desfiguración de páginas web.<br>- Manipulación de información. | - Descargas de archivos sospechosos<br>- Contactos con dominios o direcciones IP sospechosas<br>- Escáneres de vulnerabilidades.<br>- Códigos dañinos de bajo impacto (adware, spyware, etcétera).<br>- Sniffing.<br>- Ingeniería social. | - Capacidad para filtrar un volumen identificado de información.<br>- Capacidad para tomar el control de algún sistema. |
| **BAJO** | - Ataques a la imagen.<br>- Errores y fallos.<br>- Políticas. | - Spam sin adjuntos.<br>- Software desactualizado.<br>- Acoso, coacción, comentarios ofensivos.<br>- Error humano. | - Escasa capacidad para filtrar volumen de información.<br>- Nula o escasa capacidad para tomar el control de sistemas. |

Fuente: propia

## IDENTIFICACIÓN DE LA CULTURA DE CONTROL EN CIBERSEGURIDAD POR PARTE DE LA DIRECCIÓN

Según la Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA)

> El concepto de Cultura de Ciberseguridad (CSC) se refiere al conocimiento, creencias, percepciones, actitudes, suposiciones, normas y valores de las personas con respecto a la ciberseguridad y cómo se manifiestan en el comportamiento de las personas con las tecnologías de la información. (ENISA, 2017, Cyber Security Culture in Organitations)

En el marco de la evaluación de riesgos, deberíamos comprender los métodos utilizados por la empresa para prevenir y detectar incidentes cibernéticos que puedan tener un efecto material en los estados financieros y así como evaluar y abordar incidentes cibernéticos materiales, una vez identificados. Esto incluye comprender, por ejemplo, cómo la dirección garantiza la evaluación oportuna y la presentación de informes de incidentes cibernéticos, cómo la empresa garantiza la derivación adecuada a los accionistas y la consideración oportuna de divulgación a los inversores y otros usuarios interesados.

Más allá de no haber identificado un incidente de seguridad cibernética específico, es importante que como auditores nos mantengamos profesionalmente escépticos y alertas durante la toda la auditoría, ya que según estudios el tiempo medio para identificar una infracción es de aproximadamente 196 días (Cyber Security Culture in Organizations, s.f.) y, por lo tanto, existe una posibilidad real de que se haya producido una filtración y aún no se haya identificado o comunicado al equipo del encargo.

En aquellos casos donde una empresa es víctima de un ciberataque, debemos evaluar la naturaleza y el alcance de la filtración, incluido lo que fue robado, alterado o destruido. También considerar el efecto esperado del incumplimiento en las operaciones de la empresa. En estos casos, deberíamos contar con herramientas para abordar las implicancias económicas, financieras (pérdida de ingresos, costos asociados a readecuación, sustracción de activos) y de presentación en los estados financieros en relación con el hecho detectado. Adicionalmente, debemos evaluar si el incidente fue producto de una deficiencia en los controles internos de la empresa y si ha implementado procedimientos para prevenir incidentes similares en el futuro.

Por otra parte, dado que la responsabilidad del auditor continúa durante toda la auditoría, si antes de la firma de nuestro informe se obtiene información sobre un incidente cibernético, debemos evaluar si dicho ataque tiene consecuencias en la planificación de nuestro trabajo. De ser así, podríamos revisar la evaluación de riesgos y modificar apropiadamente los procedimientos de auditoría y realizar otros adicionales, como también evaluar de acuerdo con la información obtenida si este hecho identificado con posterioridad a la fecha de cierre de ejercicio tiene impacto sobre los estados financieros.

Nuevos alcances de trabajos para los profesionales. Todas las partes interesadas de las empresas (empleados, proveedores, clientes, gobierno, etc.), conocidos como stakeholders, están presionando cada vez más para que las organizaciones demuestren que están gestionando las amenazas a la ciberseguridad, y que han puesto en marcha programas de gestión de riesgos para prevenir, detectar y responder a estos riesgos. El 62% de los gerentes ejecutivos esperan que se incrementen las solicitudes de los directorios de las compañías sobre la implementación y eficacia de programas de ciberseguridad (Deloitte, s.f.). En línea con esto, algunas firmas de auditoría hemos comenzado a requerir por parte de las empresas, asesoramientos para el desarrollo de un sistema de gestión de riesgos relacionados con ciberseguridad o encargos de aseguramiento sobre el funcionamiento de sistemas de gestión de riesgos de ciberseguridad ya implementados. En cuanto a este último, el profesional idóneo proporcionaría una conclusión sobre la descripción de la gerencia del programa de gestión de riesgos de ciberseguridad de la entidad y la efectividad de los controles, para alcanzar los objetivos de ciberseguridad de la entidad.

En el caso de los servicios de asesoramiento, normalmente

se forman equipos interdisciplinarios con profesionales del área de tecnología de la información (IT por sus siglas en ingles), contadores y abogados expertos en cibercrimen, quienes abordan los potenciales riesgos a los que está expuesta la organización y proporcionan una serie de recomendaciones para mejorar y desarrollar su sistema de gestión de riesgos de ciberseguridad. En este marco, los objetivos son: 1) Reducir la probabilidad de ocurrencia. 2) Tomar medidas rápidas para detectar un ataque. 3) Preparar a la organización en caso de un ataque. 4) Maximizar la resiliencia de la organización ante un ataque cibernético destructivo. Algunas de estas recomendaciones pueden estar relacionadas con la implementación de normas de calidad ISO 27001 sobre el manejo de la seguridad de información, con la implementación de controles sobre áreas de riesgos sin controles asociados o la flexibilización de otros controles para poder adaptarlos a todas las áreas de la organización.

Otro servicio relacionado, y no menos importante si consideramos la tendencia a la digitalización de la información, es la elaboración de informes de controles de organizaciones de servicios (SOC por sus siglas en inglés). El uso intensivo de la tecnología para el manejo de información sensible digitalizada compartida en la nube con las organizaciones de servicios, las ha obligado a implementar controles adecuados para garantizar la seguridad, confidencialidad, disponibilidad y la integridad de toda la información de terceros que gestiona.

AICPA ha publicado guías para el desarrollo de estos trabajos que solo pueden ser emitidos por auditores o firmas de auditores por este organismo certificadas. Principalmente hay 3 tipos de informes mencionadas por dicho instituto (AICPA, s.f.):

**SOC 1:** están destinados específicamente a satisfacer las necesidades de las entidades que utilizan organizaciones de servicios (entidades usuarias) y los auditores de los estados financieros de las entidades usuarias (auditores de los usuarios), en la evaluación del efecto que los controles en la organización de servicios tienen o no impacto sobre los estados financieros de las entidades usuarias.

**SOC 2:** evalúa de manera independiente todo lo referente a los controles operativos y se focaliza especialmente en la seguridad, la disponibilidad, la integridad de los procesos, la confidencialidad y la privacidad. También suele incluir una opinión del auditor acerca del diseño y el funcionamiento de los controles definidos por la compañía. Particularmente, este informe se ha convertido en el último tiempo en un estándar de internacional para evaluar las amenazas de ciberseguridad.

**SOC 3:** estos informes están diseñados para satisfacer las necesidades de los usuarios que necesitan garantías sobre los controles en una organización de servicios relacionados con la seguridad, la disponibilidad, la integridad del procesamiento, la confidencialidad o la privacidad, pero que no tienen la necesidad o el conocimiento necesarios para hacer un uso efectivo de un Informe SOC 2.

## CONCLUSIÓN

Los ciberdelitos representan una de las amenazas económicas, operativas y de seguridad más importantes de nuestro tiempo. Afecta tanto a empresas, inversores como organismos de control; nosotros, como auditores externos, no quedamos ajenos al problema.

En este sentido, la planificación de nuestro trabajo y el análisis de riesgos relacionados con ciberseguridad deberían comenzar a ocupar un lugar en nuestra evaluación de riesgos, lo que nos permitiría enfocar parte de nuestros esfuerzos en analizar con qué probabilidad pueden ocurrir inconvenientes de ciberseguridad y cuál sería su impacto en los estados financieros. Asimismo, deberíamos solicitar a los entes auditados validaciones de seguridad tanto internas como externas, realizadas por profesionales idóneos como así también la adherencia a estándares internacionales en lo referente a ciberdelitos.

Además de esto, y como un valor agregado a nuestros clientes, debemos adentrarlos en la problemática de la situación, alertarlos en la subestimación de las consecuencias e informarles al comienzo de nuestro trabajo que, como auditores externos, debemos evaluar los riesgos asociados y cómo la empresa implementa y ejecuta controles para mitigar estos riesgos. Esta situación también puede abrir puertas a nuevas posibilidades de servicios.

En el ámbito local, será de suma importancia el rol de los organismos reguladores, tanto de empresas como de profesionales, y la rigurosidad con la que implementen sus planes, procedimientos y responsabilidades tendientes a mitigar riesgos de ataques cibernéticos en búsqueda de proteger los intereses de los stakeholders. En Argentina, el Banco Central, como ente regulador de las entidades financieras, es uno de los primeros organismos que ha comenzado a tomar un rol activo en este tema, publicando resoluciones que, aunque tienen el carácter de recomendación y no de obligatoriedad, intentan guiar a sus empresas reguladas para que trabajen sobre temas tendientes a identificar, analizar, comunicar y mitigar riesgos de ciberseguridad. Para desarrollar estos planes, los organismos podrán tomar como ejemplo alguna de las medidas puestas en práctica en Estados Unidos y Europa, que si bien cuentan con aspectos a revisar, han avanzado con la intervención de empresas cotizadas víctimas de ciberdelitos, evaluando si la información brindada a sus inversores es la suficiente y si sus procesos de detección son los adecuados. Sin embargo, este es solo el puntapié inicial de un gran camino por recorrer. Los auditores externos ocupamos un rol importante, ya sea como nexo entre dichos organismos y las empresas, pues asesoramos para implementar procesos internos, o como sujetos obligados a verificar el cumplimiento de las empresas. En cualquier caso, implica que debemos prepararnos y estar a la vanguardia para nuevas exigencias.

## REFERENCIAS

Accenture (2018). *From Bottom Line to Front Line* (Archivo PDF), p. 13. https://www.accenture.com/t20180910T083815Z__w__/us-en/_acnmedia/PDF-85/Accenture-CFO-Research-Global.pdf

American Institute of Certified Public Accountants (s.f). En *System of Control for Cybersecurity.* Recuperado de https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurityforcpas.html.

American Institute of Certified Public Accountants (s.f). *SOC for Service Organizations.* https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.

Computer Security Resource Center (s.f). Cyber Attack. En *Computer Security Resource Center's Glossary.* Recuperado de https://csrc.nist.gov/glossary.

Deloitte (s/f). *Corporate Boards May Be More Likely Than Regulators to Scrutinize Cybersecurity Program Effectiveness This Year.*

European Union Agency For Network and Information Security (2017). *Cyber Security Culture in Organizations.*

Information Systems Audit and Control Association (s.f). Cybersecurity. En *Information Systems Audit and Control Association´s Glossary of terms.* Recuperado de https://www.isaca.org/resources/glossary.

NIA 315 (Revisada en 2019). International Auditing and Assurance Standards Boar*,* parr. A224.

NIA 400. International Auditing and Assurance Standards Board, Sistemas de contabilidad y control interno.

NIA 720 (Revisada en 2020). International Auditing and Assurance Standards Board, parr. 11.

Ponemon Institute LLC (2018). *Cost of a Data Breach Study: Global Overview,* p. 33.

Reuters (2021). *Wide-Ranging SolarWinds Probe Sparks Fear in Corporate America.* https://www.reuters.com/technology/exclusive-wide-ranging-solarwinds-probe-sparks-fear-corporate-america-2021-09-10/

Securities Exchange Commission (2018). *Accounting and Auditing Enforcement Release No. 3937* (Archivo PDF). https://www.sec.gov/litigation/admin/2018/33-10485.pdf