UNIVERSIDAD DE Belgrano

BUENOS AIRES - ARGENTINA

Facultad de Ciencias Económicas

TESINA

# La Auditoria Interna y su Responsabilidad frente al Ciberdelito en tiempos de Covid

Período 2020-2021


Alumno: Cambiasso Deleau, Nicolás

ID: 04-9557

Carrera: Contador Público (301)

E-mail: nicolas.cambiasso@comunidad.ub.edu.ar

Turno: Mañana

Tutor: Profesora, Leticia Bonfiglio (Legajo 30198)

# INDICE

## ABSTRACT

El presente trabajo buscará dar a todas aquellas personas que lo lean, las distintas herramientas con las que cuenta y debe contar el sector de Auditoria Interna de los distintos tipos de Organizaciones para prevenir y controlar este delito, en este periodo excepcional que estamos transitando de pandemia, donde el aumento del Ciberdelito y las distintas prácticas de fraude, partiendo del contexto actual que se presta a que con mayor facilidad todas aquellas organizaciones criminales dedicadas a este tipo de estafas vean los distintos mecanismos para llevar a cabo su cometido.
En un primer capítulo se mencionaran todos aquellos conceptos y características relacionadas con el Ciberdelito y cuáles son los mecanismos utilizados por la Auditoria Interna para la prevención de este tipo de delitos.

En el segundo capítulo se explicaran las distintas Normativas tanto Nacionales como Internacionales dedicadas al control y prevención del Ciberdelito, donde la auditoria interna debe recurrir para mitigar este flagelo que azota a todas las organizaciones.

Y por último en el tercer capítulo, se tendrá en cuenta cual es la responsabilidad del Auditor Interno frente al Ciberdelito y se tendrán opiniones de fuente primaria de dos Profesionales quienes nos comentaran sus experiencias personales en este tiempo de Covid y su trabajo profesional.

## INTRODUCCION

El avance de las nuevas tecnologías ha propiciado un cambio sin precedentes que ha influido en la forma de operar de las organizaciones, cuyas actividades se desarrollan cada vez más en el ciberespacio.

Este hecho propicia un gran desarrollo económico y social, pero a la vez la aparición de nuevos retos y amenazas que es imprescindible gestionar. No en vano el Foro Económico Mundial incluye varios riesgos asociados a la ciberseguridad en su ranking de Riesgos Globales desde hace años.

Los Ciberdelitos han ido creciendo vertiginosamente llevando a las Organizaciones a invertir cada vez más dinero en tecnologías que puedan frenar la fuga de divisas con

estos actos delictivos, para dar un ejemplo en Europa en el año 2019 el coste medio de un ataque informático les representa a las organizaciones una pérdida de 115.000 euros y en la Argentina donde las tecnologías no son tan complejas como en el viejo continente, aun es más vulnerable los sistemas de Seguridad.

Los ciberataques y su naturaleza se han multiplicado en los últimos años, y cada vez son más complejos y más difíciles de prevenir y detectar, lo que hace que los órganos de gobierno de las organizaciones deban incrementar y mejorar la supervisión sobre la Ciberseguridad.

“Las personas y las organizaciones en todo el mundo están luchando para superar la crisis provocada por la pandemia COVID-19 y sus efectos tanto directos como colaterales; en esa lucha, los auditores internos son la parte activa, ayudando a las organizaciones a superar la crisis y recuperarse de la misma”. Según Nelson, L. (2020). “Modelo para gestionar el riesgo de fraude corporativo durante una Pandemia”, de Instituto de Auditores Internos de Argentina.

Es por todo esto, con el presente trabajo se buscara describir aquellos conocimientos y herramientas tecnológicas que en la actualidad pueden tener a su alcance las organizaciones, para que la auditoria interna las aplique en la prevención y control de esta actividad que viene en aumento en este contexto de pandemia. Tratando de disminuir el riesgo y así llevar más tranquilidad a sus clientes.

**PALABRAS CLAVES:** CIBERDELITO, AUDITORIA INTERNA, PANDEMIA, CONTADOR PUBLICO, CIBERSEGURIDAD.

**CIBERDELITO:**

“El concepto de riesgo cibernético o Ciberdelito proviene de la amenaza continua y a escala industrial sobre los activos digitales, las operaciones y la información corporativa, por parte de terceros”. Según el Instituto de Auditores Internos de España.

“En líneas generales, cuando se habla de delitos informáticos nos referimos a aquellas conductas indebidas e ilegales donde interviene un dispositivo informático como medio

para cometer un delito o como fin u objeto del mismo. En este sentido, los delitos informáticos son entendidos respecto al lugar que ocupa la tecnología para la comisión del delito más que a la naturaleza delictiva del acto mismo". Edwind Sutherlard (1929)

**PANDEMIA:**

Según la Organización Mundial de la Salud, se llama pandemia a la propagación mundial de una nueva enfermedad. Se produce una pandemia de gripe cuando surge un nuevo virus gripal que se propaga por el mundo y la mayoría de las personas no tienen inmunidad contra él. Por lo común, los virus que han causado pandemias con anterioridad han provenido de virus gripales que infectan a los animales. Fuente: OMS. (2016)

**CONTADOR PÚBLICO:**

"El Contador debe ser un Profesional con saberes contables consistentes, dotado de una fuerte formación jurídica, principalmente en las áreas de su incumbencia (derecho comercial, sucesiones, tributario, laboral, procesos concursales, entre otros), un experto en el manejo de herramientas de administración, informáticas y financieras, con capacidad de análisis en temas económicos de aplicación en la micro y macro economía, dotado de un espíritu crítico, organizativo y de control, con un desarrollo de técnicas para el manejo de personal y preparado para la toma de decisiones, o en su caso, brindando un adecuado asesoramiento que permita a otras personas decidir apropiada y oportunamente." Tkaczek (2009)

**CIBERSEGURIDAD:**

"También conocida como seguridad de las tecnologías de la información, es la rama de la informática que procura detectar vulnerabilidades que ponen en juego la integridad, disponibilidad y confidencialidad de los sistemas informáticos". https://nic.ar/es/enterate/novedades/que-es-ciberseguridad

## PREGUNTA DE INVESTIGACION

Dada la pandemia que estamos atravesando a nivel mundial, el avance continuo de la tecnología y la globalización de las Organizaciones, me surge el siguiente interrogante:

¿Cuál es la Responsabilidad de la Auditoria Interna frente al Ciberdelito en tiempos de Covid?

## OBJETIVO GENERAL

Analizar los diferentes factores que llevan al Ciberdelito, a ser una de las principales amenazas para las Organizaciones en tiempos de Covid.

## OBJETIVO ESPECIFICO

- Realizar una descripción de los conceptos que se utilizan para el Ciberdelito, sus características y las diferentes modalidades utilizadas para llevar adelante estos delitos.
- Plantear el marco teórico-normativo con el que cuenta la Auditoria Interna para el Ciberdelito en las Organizaciones.
- Entender cuál es la responsabilidad del Contador Público como Auditor Interno frente a este tipo de delitos en Pandemia.

## MARCO TEORICO

El Marco Teórico es el soporte conceptual de diferentes niveles de abstracción articulados entre sí que orientan la forma de aprehender la realidad. Incluye supuestos de carácter general acerca del funcionamiento de la sociedad y la teoría o conceptos específicos sobre el tema que se pretende analizar. En dicho trabajo se utilizara para poder alcanzar los objetivos planteados, distintas fuentes de información vinculadas al tema, que son las siguientes:

- Para el desarrollo del trabajo Final de Carrera se utilizara la Bibliografía

correspondiente al autor Nelson L. “Modelo para gestionar el riesgo de fraude corporativo durante una Pandemia”, de Instituto de Auditores Internos de Argentina publicada en el año 2020. Donde claramente podemos destacar su visión sobre el Ciberdelito, las distintas formas que se puede presentar este tipo de ilícitos y que herramientas utiliza la auditoria interna para tratar de prevenir y controlar la gran cantidad de operaciones de este tipo que todos los días se intentan llevar a cabo en pandemia.

- Otro de los referentes de la Auditoria que no podemos dejar de consultar es el autor Slosse C. donde en su edición N° 3 del libro “Auditoria” contamos con un material enriquecedor desde lo técnico-practico para la auditoria interna.
- Se utilizaran las 5 principales leyes sobre la materia objeto de investigación que a continuación pasaremos a detallar: **Ley de Protección de Datos Personales (Ley 25326), Ley de Propiedad Intelectual (Ley 11.723)**, **Ley de Delitos Informáticos (Ley 26.388)**, **Ley de Grooming (Ley 26.904) y Ley 27.411. Aprobación del Convenio sobre Ciberdelito (Convenio de Budapest sobre Ciberdelito)**.
- Para el trabajo de campo se recurrirá a la experiencia en primera persona de dos Profesionales en la Materia de Auditoria Interna y el flagelo que compromete a las organizaciones a través del ataque cibernético. Los Contadores Dr. Nicolás Patricio Rocca – Socio de la empresa **MAKINGPROGRESS S.A.** y Dra. Patricia Russo – de la empresa **SERRA RICCO S.A.**

## METODOLOGIA

La Metodología no es una ciencia, es el estudio del método, el método es el camino para llegar a las soluciones que buscamos o pretendemos encontrar, comúnmente llamado objetivo de la investigación. Para tener una mejor comprensión de la conclusión que vamos a describir de acuerdo al marco metodológico que le daremos a nuestra tesina, es importantísimo tener claro el método a utilizar.

La metodología que se utilizara en la siguiente investigación será de carácter cualitativo, ya que se buscó describir, comprender e interpretar los fenómenos. El criterio que se utilizó para las entrevistas a los distintos Contadores Públicos, no se realizó con la

intención de obtener datos sujetos a probabilidades, sino que fue orientado a datos por propósitos.

## Procedimiento Metodológico:

En primer lugar, identificaré las variables conceptuales objeto de estudio.

En segundo lugar, recopilaré datos de cada variable, teniendo en cuenta la fuente más adecuada y representativa para describirla.

Por último, con la información obtenida, utilizaré el método inductivo, donde realizaré las conclusiones de las variables que fueron objeto de análisis.

## Recolección de Datos:

### Fuentes Primarias:

**Entrevistas a Expertos:** se realizaron entrevistas abiertas a Contadores Públicos con amplio conocimiento en el Sector de Auditoria Interna, con el objetivo de recopilar información sobre las variables objeto de estudio.

### Fuentes Secundarias:

**Material Bibliográfico:** consultaré Libros de los principales referentes nacionales en materia de Auditoria Interna, Ciberdelitos y Fraude Corporativo como Auditoria Tercera Edición (Carlos Alberto Slosse) y Nelson, L. (2020). “Modelo para gestionar el riesgo de fraude corporativo durante una Pandemia”, de Instituto de Auditores Internos de Argentina

**Publicaciones Periódicas:**

**Páginas WEB:** se recurrió a información páginas web de Entidades como Infoleg y sitios de publicaciones periodísticas sobre actualidad en materia de la relación entre el Ciberdelito y el Covid.

# CAPITULO 1: El Ciberdelito, sus características y herramientas para combatirlo.

## 1.1Que entendemos por Ciberdelito

Las tecnologías de la información y las comunicaciones (TIC) propician el desarrollo económico de la sociedad de manera integrada dentro de las empresas y organizaciones, que usan en su actividad el amplio abanico de dispositivos electrónicos y redes de comunicaciones disponibles.

Sin embargo, de la mano de dicha expansión tecnológica y el aumento del uso de servicios de Internet surgen nuevos retos y desafíos para las organizaciones. Así, una de las principales amenazas que han traído consigo estos avances es la proliferación de acciones delictivas en el ciberespacio.

Entonces podemos definir al Ciberdelito como: Conductas ilegales realizadas por ciberdelincuentes en el ciberespacio a través de dispositivos electrónicos y redes informáticas. Son estafas, robo de datos personales, de información comercial estratégica, robo de identidad, fraudes informáticos, ataques como cyberbulling, grooming, phishing cometidos por ciberdelincuentes que actúan en grupos o trabajan solos

## 1.2 Ciberdelito – Caracteristicas

Los Medios comúnmente utilizados son los siguientes:

- Internet
- Computadoras
- Celulares
- Redes de Comunicación 3G, 4G y 5G
- Redes de fibra óptica y software.

Otra de las principales características que tienen este tipo de ataques es la utilización de programas maliciosos desarrollados para borrar, dañar, deteriorar, hacer inaccesibles, alterar o suprimir datos informáticos sin tu autorización y con fines económicos y de daño.

Algunos ejemplos son:

- Ataques en tu navegación: desvían tu navegador hacia páginas que causan infecciones con programas malignos como virus, gusanos y troyanos. Estos programas pueden borrar tu sistema operativo, infectar tu teléfono y tu computadora, activar tu webcam, extraer datos, etc.

- ataques a servidores: pueden dañar o robar tus datos y negarte el acceso a tu información.

- corrupción de bases de datos: interfieren en bases de datos públicas o privadas para generar datos falsos o robar información.

- virus informáticos: encriptan archivos, bloquean cerraduras inteligentes, roban dinero desde los celulares con mensajes de texto que parecen de la compañía,

- programa espía: alguno de los dispositivos tiene instalado un software que le permite encender y grabar con la cámara y el micrófono. También puede acceder a tu información personal sin autorización y sin que lo sepas.

Los ciberdelitos que usan la ingeniería social para engañarte, amenazarte y sacarte datos personales o información de otras personas u organizaciones, sacarte dinero, suplantar tu identidad, acosarte digital y sexualmente.

Algunos ejemplos son:

- **Phishing o Vishing:** los ciberdelicuentes se hacen pasar por empresas de servicios, oficinas de gobierno o amigos de algún familiar y te piden los datos que les faltan para suplantar tu identidad y así operar tus cuentas en bancos, perfiles en las plataformas y redes sociales, servicios y aplicaciones web.

- **Fingerprinting:** búsqueda y recolección de todo tipo de información del objetivo, principalmente en Internet, y realizada de manera pasiva, que pueda ser utilizada en la perpetración de un ataque. Puede incluir tanto la recolección de información de fuentes públicas (OSINT: Open-Source Intelligence), como de fuentes privadas o de pago.

- **Enumeración y Escaneo:** identificación de sistemas, equipos y dispositivos existentes en la red. Obtención de nombres de equipos, usuarios, recursos compartidos, etc. También incluye habitualmente la identificación de posibles vulnerabilidades.

- **APT (Amenaza Persistente Avanzada):** ataques especialmente diseñados y dirigidos contra una organización o entidad concreta. Por lo general requieren de un elevado tiempo de preparación y combinan diferentes técnicas y vulnerabilidades de entre las ya comentadas anteriormente.

- **Grooming:** se trata de personas adultas que, de manera velada, intentan obtener fotografías o videos sexuales de personas menores para posteriores chantajes o previo al abuso sexual.

- **Ciberodio:** son contenidos inapropiados que pueden vulnerar personas. Se considera ciberodio a la violencia, mensajes que incitan al odio, la xenofobia, el racismo y la discriminación o maltrato animal.

Otra dimensión del ciberdelito tiene que ver con la violación de la privacidad de las personas:

- Espionaje ilícito sobre las comunicaciones privadas de los ciudadanos.

- Violación a la intimidad por parte de las empresas proveedoras de servicios de Internet sin el consentimiento del usuario, para conocer sus gustos y preferencias y establecer la venta agresiva de productos y servicios asociados.

- Acceso ilegal a las comunicaciones privadas de un trabajador (mails, redes sociales, etc.)

## 1.3 Principales Ciberamenzas que sufrieron las Organizaciones

Son numerosos los ataques recibidos por grandes corporaciones y multinacionales durante los últimos años, como JPMorgan, Sony, Target, Apple, Home Depot, o Google, entre otras. También administraciones públicas y gobiernos de todo el mundo están entre los damnificados que han sufrido robos de información de sus bases de datos de clientes, elevadas pérdidas económicas, prolongadas indisponibilidades en sus sistemas, daños reputacionales o sabotajes de sus servicios online; como consecuencia del denominado cibercrimen.
Sirvan como ejemplos de lo anterior las siguientes ciberamenazas que han provocado algunas de las mayores infecciones y trastornos recientes en materia de seguridad informática:

- **Zeus.** Malware orientado al robo de información personal de los usuarios: credenciales de cuentas de correo electrónico, redes sociales, datos de servicios financieros, etc.

- **Flame y Agent BTZ.** Software espía con gran capacidad de propagación capaz de obtener capturas de pantalla, pulsaciones de teclado, control del bluetooth, webcam o grabación de llamadas. Asimismo, posee la capacidad de transmitir la información recopilada ocultándola mediante técnicas de cifrado.

- **Carbanak.** Ataque Persistente Avanzado (APT) diseñado y dirigido al sector bancario, capaz de alterar y manipular el funcionamiento de las redes y software de control de los cajeros automáticos.

- **Ransomware.** También conocido como el “virus de la policía”, cifra la información contenida en el sistema del usuario infectado, solicitando una compensación

económica para su desbloqueo.

- **Stuxnet.** Software malicioso descubierto en 2010, capaz de controlar y manipular software de control y supervisión de procesos industriales (SCADA).

## 1.4 Técnicas y Herramientas contra el Ciberdelito

Una de las herramientas más efectivas y actuales contra el Ciberdelito es la Ciberseguridad, esta no debe circunscribirse a los departamentos de Tecnologías Informáticas, sino que la Alta Dirección ha de implicarse en su gestión eficiente con un compromiso activo continuo.

Por tanto la seguridad corporativa ya no se identifica únicamente con la seguridad preventiva, ni es responsabilidad exclusiva de un departamento, ni se separa en un escenario interior o exterior o con un enfoque reactivo o preventivo.

De este modo surgen en el seno de las empresas nuevas actividades y tareas relacionadas entre las que cabe destacar:

- ·Análisis de la exposición a los ciberriesgos por parte de las entidades, identificación y clasificación de información crítica existente en una organización y establecimiento de una estrategia de seguridad.

- Concientización: Cualquier persona o área de una entidad puede ser víctima de un ciberataque, por lo que resulta necesario establecer una cultura de seguridad en las organizaciones con el objetivo de cambiar la manera en que la seguridad es percibida por las personas, adoptando entre otras algunas de estas medidas:

- Divulgación de políticas y manuales de seguridad.
- Difusión de incidentes y ataques de seguridad, explicando sus causas y orígenes.

- Establecimiento de cursos y actividades formativas en materia de prevención y detección de los riesgos de ciberseguridad.

También otra de las herramientas es la toma de medidas tanto Organizativas como Técnicas.

- **Medidas organizativas:** como la difusión de políticas de seguridad en las organizaciones o la concientización a los usuarios de los riesgos en el uso de las tecnologías de la información.

- **Medidas técnicas:** que pueden incluir desde la existencia de herramientas para la gestión centralizada de alertas y eventos de seguridad en los sistemas a técnicas que permitan detectar y prevenir fugas de información confidencial; contratación de servicios de hacking ético y auditorías forenses de seguridad; búsqueda de información en Internet, prensa o redes sociales; suscripción a servicios de alertas, incidentes y vulnerabilidades de seguridad; e incluso la contratación de pólizas de los denominados ciberseguros que cubran la pérdidas ocasionadas por un ciberataque, y la participación en ciberejercicios que permitan evaluar las capacidades de organización y resiliencia ante el cibercrimen.

- **Sistemas de Seguridad:** Todos los días tenemos riegos que atentan contra la seguridad de la información, tales como usuarios internos, usuarios externos y desastres naturales.

¿Qué podemos hacer para proteger datos e información en un entorno como este?

La respuesta es simple:

♣ Se puede implementar un sistema de gestión de seguridad de la información.

¿Para qué sirve?

♣ Conocer

♣ Gestionar

♣ Minimizar los riesgos que atentan contra la seguridad de la información

¿Qué nos permite un Sistema de Gestión de Seguridad Informática?

♣ Analizar y ordenar la estructura de los sistema de información.

♣ Establecer los procedimientos de trabajo para mantener su seguridad.

♣ Disponer de controles para medir la eficacia de lo establecido en el punto anterior.

La idea es alcanzar un nivel de riesgo menor que el soportado por la institución, para preservar la confidencialidad, integridad y disponibilidad de la información.

# CAPITULO 2: Marco Teórico – Normativo

## 2.1 Principales Organismos Internacionales contra el Ciberdelito

En el ámbito Internacional caben destacar otras iniciativas como La Estrategia de Ciberseguridad de la Unión Europea (publicada en 2013), o la Directiva de Seguridad de la Redes y la Información (NIS), que establece medidas de control y mecanismos de cooperación concretos entre los estados miembros, como la red de equipos de respuesta a incidentes de seguridad (CSIRT) y el grupo de cooperación, compuesto por miembros de autoridades nacionales competentes, la Comisión de la Unión Europea y la ENISA. La Directiva también obliga a diseñar una estrategia de ciberseguridad nacional, y la obligación para empresas que trabajan en sectores críticos tales como energía, transporte y finanzas, entre otros, a informar a las autoridades nacionales acerca de incidentes de impacto significativo.

Se ha establecido que las 5 estrategias prioritarias a desarrollar son:

- La resiliencia contra ciberataques.
- La reducción drástica de la delincuencia en la red.
- El desarrollo de una política de ciberdefensa y de las capacidades correspondientes en el ámbito de la Política Común de Seguridad y Defensa (PCSD).
- El desarrollo de los recursos industriales y tecnológicos necesarios en materia de ciberseguridad.
- El establecimiento de una política internacional coherente del ciberespacio en la Unión Europea y la promoción de los valores europeos esenciales.

Así pues, son numerosas las iniciativas a nivel internacional que diferentes organismos, reguladores y gobiernos están promoviendo en el ámbito de la ciberseguridad y

protección de las infraestructuras críticas, entre las que cabe destacar la aprobación y promulgación de diversas leyes en diferentes países:

- **Cybersecurity Enhancement Act of 2014 (Estados Unidos**). Proporciona una asociación permanente público-privada para mejorar y fortalecer la investigación y el desarrollo del personal, educación, preparación y conciencia en materia de ciberseguridad.
- **Cybersecurity Act of 2015 (Estados Unidos)**. Creada con el objetivo de promover y alentar al sector privado y gobierno de Estados Unidos para intercambiar con rapidez y de manera responsables información sobre las amenazas cibernéticas.
- **IT Security Act (Alemania)**. En respuesta, y tras la alarma del ciberataque al parlamento alemán (Bundestag) conocido en junio de 2015, Alemania aprobó una ley de seguridad informática destinada a reforzar los dispositivos de protección a las empresas, debiendo además informar de inmediato acerca de cualquier incidente, anomalía o sospecha de virus.

## 2.2 Normas ISO 27000

Contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de Seguridad Informática:

♣ ISO/IEC 27000 - es un vocabulario estándar para el SGSI. (en desarrollo actualmente).

♣ ISO/IEC 27001 - es la certificación para las organizaciones. Especifica los requisitos para la implantación del SGSI. La más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.

♣ISO/IEC 27002 - es código de buenas prácticas para la gestión de seguridad de la información.

♣ ISO/IEC 27003 - son directrices para la implementación de un SGSI.

♣ ISO/IEC 27004 - son métricas para la gestión de seguridad de la información.

♣ ISO/IEC 27005 - trata la gestión de riesgos en seguridad de la información.

♣ ISO/IEC 27006:2007 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información.

♣ ISO/IEC 27007 - Es una guía para auditar al SGSI.

♣ ISO/IEC 27799:2008 - Es una guía para implementar ISO/IEC 27002 en la industria de la salud.

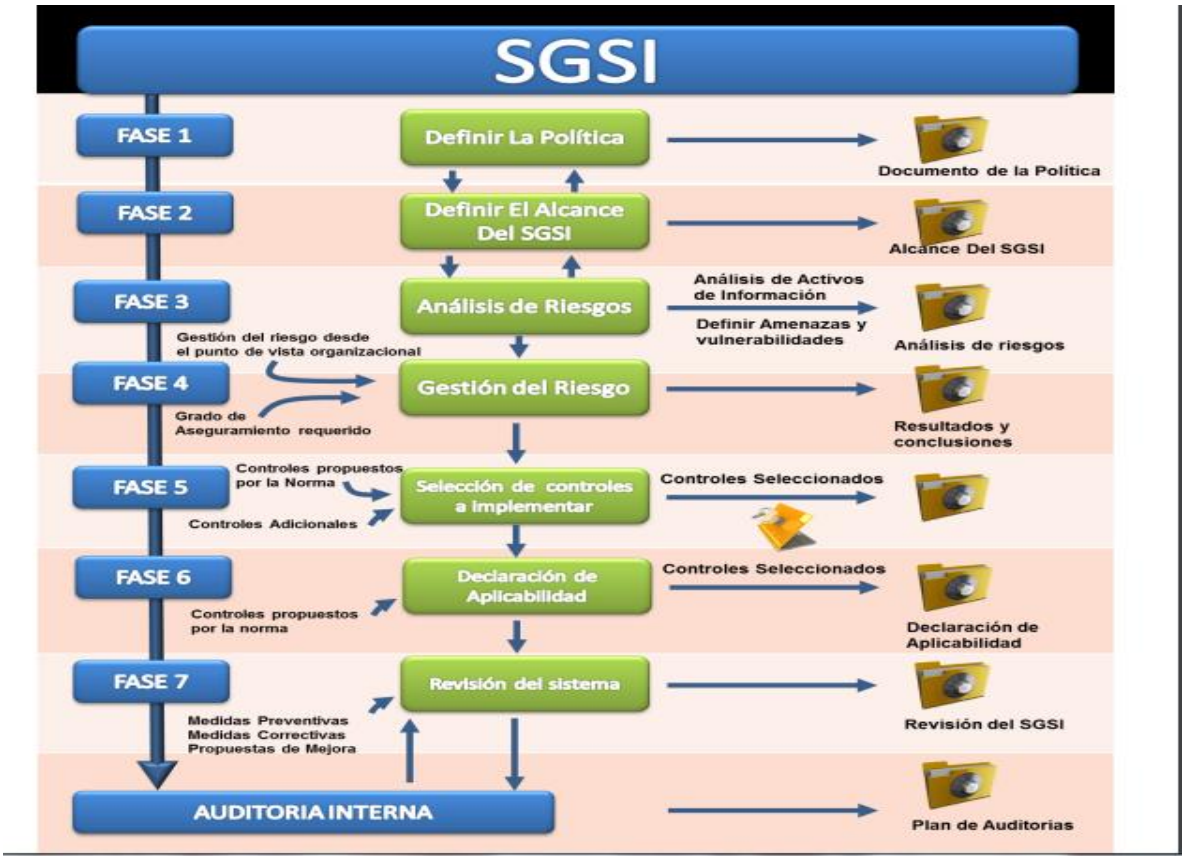
♣ ISO/IEC 27035:2011 – Técnicas de Seguridad – Gestión de Incidentes de Seguridad: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.

**Alcance de la Norma ISO/IEC 27000**

♣ ISO 27001 propone un marco de gestión de la seguridad de toda la información de la empresa, incluso si es información perteneciente al propio conocimiento y experiencia de las personas o sea tratada en reuniones etc.

♣ No debemos centrar la atención solamente en los sistemas informáticos por mucho que tengan hoy en día una importancia más que relevante en el tratamiento de la información ya que de otra forma, podríamos dejar sin proteger información que puede ser esencial para la actividad de la empresa.

**IMPLEMENTACION DEL SISTEMA**




Fuente: http://archivo.ucr.ac.cr/docum/ISOEIC27000

## 2.3 Principales Organismos Nacionales contra el Ciberdelito

A nivel mundial, cuando se habla de **"delito informático"** se implican actividades criminales que los países han tratado de encuadrar en figuras de carácter tradicional, tales como robos, hurtos, fraudes, estafas y sabotajes. En algunos países, como Argentina, esto generó que no se creen nuevas leyes, sino que se fueran modificando. De manera general, podríamos decir que existen cinco leyes que se encargan de enmarcar distintas figuras delictivas del mundo digital:

1. Ley de Protección de Datos Personales (Ley 25326): Se caracteriza por definir principios generales relativos a la protección de datos. Esto abarca desde derechos de los titulares hasta las figuras de usuarios y responsables de archivos,

registros y bancos de datos. El control, las sanciones, la acción de protección de los datos personales e inclusive el spam están vinculados a esta Ley.

2. Ley de Propiedad Intelectual (Ley 11.723): Establece el régimen legal de la propiedad intelectual, es decir, actúa sobre las obras científicas, literarias y artísticas. Además, comprende los "escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto".

3. Ley de Delitos Informáticos (Ley 26.388): Esta no es una ley especial que regula este tipo de delitos en un cuerpo normativo separado del Código Penal con figuras propias y específicas, sino una ley que modifica, sustituye e incorpora figuras típicas a diversos artículos actualmente en vigencia, con el objeto de regular las nuevas tecnologías como medios de comisión de delitos previstos en el Código. Principalmente incluye temas como:

    - Distribución y tenencia con fines de distribución de pornografía infantil
    - Violación de correos electrónicos
    - Acceso ilegítimo a sistemas informáticos
    - Daño informático y distribución de códigos maliciosos
    - Interrupción de comunicaciones o DOS

4. Ley de Grooming (Ley 26.904): Esta ley sancionada en noviembre de 2013, tras una intensa campaña de organizaciones a favor, pena un delito que sigue en alarmante aumento. Según su Artículo 1°, que se incorporó como artículo 131 al Código Penal: "Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma".

5. Ley 27.411. Aprobación del Convenio sobre Ciberdelito (Convenio de

Budapest sobre Ciberdelito): "El Convenio se firmó el 23 de noviembre de 2001 y entró en vigor el 1° de julio de 2004, en la ciudad de Budapest, República de Hungría. Se trata del primer tratado internacional creado con el objetivo de proteger a la sociedad frente a los delitos informáticos y los delitos en Internet**,** mediante la elaboración de leyes adecuadas, la mejora de las técnicas de investigación y el aumento de la cooperación internacional. En la actualidad, el Convenio ha sido ratificado por más de 50 naciones de todo el mundo". Según https://nic.ar/es/enterate/novedades/que-es-convenio-budapest.

"El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley":

**ARTÍCULO 1°.-** "Apruébese el CONVENIO SOBRE CIBERDELITO del CONSEJO DE EUROPA, adoptado en la Ciudad de BUDAPEST, HUNGRÍA, el 23 de noviembre de 2001, que consta de CUARENTA Y OCHO (48) artículos cuya copia auténtica de su traducción al español así como de su versión en idioma inglés, como ANEXO I, forma parte de la presente" LEY 27.411, BUENOS AIRES, 22 de Noviembre de 2017, Boletín Oficial, 15 de Diciembre de 2017, Vigente, de alcance general..

# CAPITULO 3: La Responsabilidad de la Auditoria Interna – Trabajo de Campo sobre el mismo.

## 3.1 El Rol de la Auditoria Interna

La ciberseguridad suscita mucho interés en los órganos de gobierno (comités o consejos directivos, comisiones de auditoría, comités de riesgos, etc…) de las distintas organizaciones, independientemente de su sector y actividad, y cada vez está más presente en las reuniones y en el día a día de dichos órganos.
Los riesgos derivados de ciberseguridad como fugas de información, fraudes, sabotajes, etc., pueden golpear duramente la reputación de las compañías, castigar económicamente en forma de sanciones y pérdidas, o pueden llegar a parar la operativa o prestación del servicio de las compañías, incluso en países con una regulación avanzada pueden conllevar condenas penales.

Tanto el volumen como el impacto de las amenazas están aumentando exponencialmente en los últimos tiempos. Por todo esto hay que extremar las medidas en materia de ciberseguridad y establecer todos los controles necesarios para poder mitigar los riesgos en las organizaciones.

Una buena aproximación puede consistir en integrar la ciberseguridad en el sistema comúnmente implantado en la mayoría de las organizaciones (modelo de las tres líneas de defensa).

## La primera línea de defensa

La primera línea de defensa es la propietaria de los riesgos y de su tratamiento en primera instancia. Debe realizar los procedimientos de control interno y de gestión de riesgos en su actividad diaria y tomar las decisiones en cuanto al riesgo con base a su cuantificación cualitativa y cuantitativa, con el objetivo de alcanzar los niveles óptimos en cuanto al coste/ beneficio de asumir o no un riesgo.

Debe poner en funcionamiento todas las medidas técnicas y organizativas necesarias. Los empleados y usuarios (o los propietarios de las aplicaciones sean o no desarrolladas internamente por la organización) deben ser conscientes de que son parte primordial de esta primera línea de defensa. Son el primer objetivo y la puerta de entrada más débil para los “malos”.

Deben tener mucho cuidado con correos electrónicos sospechosos, dispositivos móviles, redes Wifi, redes sociales, etc. Un uso adecuado de los mismos y conforme a las políticas de seguridad de la compañía provee una garantía que minimiza el riesgo existente. Pero esto no es suficiente, también se tienen que implantar todas las medidas técnicas (firewall, IDS, gestión de accesos, cifrado de la información, etc.) al alcance de la organización y en consonancia con la información que se maneja.

## La segunda línea de defensa

La segunda línea de defensa puede estar compuesta por diferentes funciones en la organización tales como Gestión de Riesgos de TI, Seguridad de Sistemas, Cumplimiento Normativo de TI, Asesoría Jurídica, etc. Es evidente que dependiendo de la organización unas tendrán más presencia que otras, pero todas ellas deberían tener en cuenta la ciberseguridad y sus riesgos.

La relación entre todas ellas debe formar un modelo de aseguramiento en ciberseguridad que facilite que los riesgos y controles en este ámbito se manejen de manera consistente,

mediante revisiones proactivas de la seguridad y procesos de detección, corrección y mejora continua, proveyendo de tranquilidad y confianza a la alta dirección de la organización.

Como principales tareas debe:

· Desarrollar e implementar las políticas generales (ciberseguridad) y facilitar el desarrollo e implantación del marco general de riesgos y controles.

· Establecer las metodologías y métricas para evaluar y monitorizar el proceso.

· Reforzar los marcos de control definidos por la primera línea de defensa.

· Proveer de un mapa de riesgos completo y actualizado de la organización.

· Realizar el seguimiento de la exposición al riesgo y verificación de que está dentro de los márgenes y apetito al riesgo definido en la sociedad.

· Establecer los sistemas de reporting vertical y horizontal en materia de ciberseguridad.

## La tercera línea de defensa

La tercera línea de defensa, que suele recaer sobre Auditoría Interna, en nuestro ámbito de ciberseguridad recaería más específicamente sobre Auditoría Interna de Sistemas. Debe ser completamente independiente del resto de líneas de defensa y debe proveer garantías sobre el sistema de control interno a los órganos de gobierno (consejo, comisiones de auditoría…), y la alta dirección.

Auditoría interna debe proporcionar una revisión y evaluación independiente sobre la eficacia de las líneas de defensa inferiores.

La colaboración con la segunda línea de defensa es muy importante facilitando el alineamiento con el modelo de aseguramiento a nivel corporativo y poner en contexto y elevar tanto las bondades del modelo como los gaps o deficiencias encontradas en materia de ciberseguridad.

En este punto, Auditoría Interna debería participar de manera pasiva o estar informada puntualmente de las actividades de las áreas de seguridad de sistemas (encargadas de la ciberseguridad), asistiendo a sus comités o simplemente estableciendo entre ambas una línea de reporting lo suficientemente completa.

Para definir su Plan de Auditoría, Auditoría Interna de TI debería incorporar la información suministrada por la segunda línea de defensa además de sus propios análisis prestando especial atención a la ciberseguridad.

Adicionalmente, Auditoría Interna puede participar en ejercicios de revisión técnica de la seguridad, con el fin de identificar riesgos no identificados en las capas anteriores.

A modo de guía general, el siguiente listado pretende reflejar los principales aspectos en materia de ciberseguridad, que deberían ser preocupación y objeto de revisión por parte de Auditoría Interna:

1. Colaborar con la dirección de la compañía en la creación y desarrollo de una estrategia y política de ciberseguridad.
2. Asegurar que la organización cuenta con un correcto nivel de madurez y capacidad para la identificación y mitigación de los riesgos de ciberseguridad.
3. Verificar los mecanismos para reconocer incidentes de ciberseguridad procedentes de un empleado o proveedor externo.
4. Aprovechar las relaciones con la dirección de la compañía para aumentar el nivel de concienciación con los riesgos de ciberseguridad de la Junta y el Consejo, así como su implicación y compromiso con cuestiones clave en esta materia, como la actualización de la estrategia de ciberseguridad de la compañía.
5. La ciberseguridad se encuentra formalmente cubierta e integrada en el Plan de Auditoría Interna.
6. Entender y desarrollar un perfil de riesgo en ciberseguridad de la compañía, teniendo en cuenta las nuevas tecnologías y tendencias emergentes.
7. Evaluar el programa de ciberseguridad de la compañía con el marco de ciberseguridad de la NIST, y otros estándares tales como ISO 27001 y 27002.
8. Identificar y evaluar las capacidades preventivas de control de la ciberseguridad en materia de educación, formación y concienciación de usuarios, así como procesos y herramientas de control y vigilancia digital.
9. Asegurar que la monitorización y gestión de ciberincidentes es considerada una prioridad en la compañía, existiendo un proceso de escalado claro al respecto.
10. Identificar cualquier carencia o falta de personal de IT y Auditoría Interna que pueda representar un impedimento para alcanzar los objetivos y retos de ciberseguridad de la compañía.


Fuente: * European Confederation of Institutes of Internal Auditors/Federation of Risk Management Association-2013. Endorsed by Global Institute of Internal Auditors-2014

### 3.2 El papel de Auditoría Interna en la revisión de los controles

Hay 20 controles críticos de seguridad que todas las organizaciones deberían implementar. Están alineados con el marco de ciberseguridad del NIST y son un subconjunto de los controles definidos de la publicación NIST 800-53, compendio de controles recomendados para las agencias estadounidenses, y sobre el cual se realizan las auditorías de seguridad de las agencias estatales en EEUU.

Para cada uno de los 20 enunciados, existen actividades más concretas que pueden formar parte del programa de trabajo de una auditoría de ciberseguridad.

El propio CIS cuenta con una guía para la medición de la efectividad de estos controles. Esta varía con las amenazas cambiantes. Es necesario contar con procesos de diagnóstico de la efectividad de los controles, utilizando métricas.

La automatización de estos es fundamental para alcanzar este objetivo.

Los controles están pensados para organizaciones de cualquier tipo, no obstante, el conocimiento de la organización y la exposición a las amenazas va a condicionar la propia priorización y alcance de la implantación de los controles.

| | | |
|---|---|---|
| CSC 1 | INVENTARIO DE DISPOSITIVOS AUTORIZADOS Y NO AUTORIZADOS | Gestionar activamente todos los dispositivos hardware en la red, de forma que sólo los dispositivos autorizados tengan acceso a la red. |
| CSC 2 | INVENTARIO DE SOFTWARE AUTORIZADO Y NO AUTORIZADO | Gestionar activamente todo el software en los sistemas, de forma que sólo se pueda instalar y ejecutar software autorizado. |
| CSC 3 | CONFIGURACIONES SEGURAS DE SOFTWARE Y HARDWARE PARA DISPOSITIVOS MÓVILES, PORTÁTILES, EQUIPOS DE SOBREMESA Y SERVIDORES | Establecer una configuración base segura para dispositivos móviles, portátiles, equipos de sobremesa y servidores, y gestionarlas activamente utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir a los atacantes explotar servicios y configuraciones vulnerables. |
| CSC 4 | PROCESO CONTINUO DE IDENTIFICACIÓN Y REMEDIACIÓN DE VULNERABILIDADES | Disponer un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes. |
| CSC 5 | CONTROL SOBRE PRIVILEGIOS ADMINISTRATIVOS | Desarrollar procesos y utilizar herramientas para identificar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones. |
| CSC 6 | MANTENIMIENTO, MONITORIZACIÓN Y ANÁLISIS DE *LOGS* DE AUDITORÍA | Recoger, gestionar y analizar logs de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque. |
| CSC 7 | PROTECCIÓN DEL CORREO ELECTRÓNICO Y DEL NAVEGADOR | Minimizar la posibilidad de que los atacantes manipulen a los empleados a través de su interacción con el correo electrónico y el navegador. |
| CSC 8 | DEFENSAS CONTRA EL *MALWARE* | Evitar la instalación, difusión y ejecución de código malicioso en distintos puntos, al tiempo que se fomenta la automatización para permitir una actualización rápida en la defensa, recopilación de datos y la corrección. |
| CSC 9 | LIMITAR Y CONTROLAR LOS PUERTOS DE RED, PROTOCOLOS Y SERVICIOS | Gestionar el uso de puertos, protocolos y servicios en los dispositivos que tengan red para reducir las vulnerabilidades disponibles a los atacantes. |
| CSC 10 | CAPACIDAD DE RECUPERACIÓN DE DATOS | Disponer procesos, metodologías y herramientas adecuadas para respaldar la información crítica y realizar pruebas de recuperación. |
| CSC 11 | CONFIGURACIONES SEGURAS DE DISPOSITIVOS DE RED *(FIREWALLS, ROUTERS* Y *SWITCHES)* | Establecer una configuración base para los dispositivos de infraestructura de red, y gestionarlas activamente utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir a los atacantes explotar servicios y configuraciones vulnerables. |
| CSC 12 | DEFENSA PERIMETRAL | Desarrollar una estrategia para detectar, prevenir y corregir los flujos de transmisión de información entre redes de distintos niveles de seguridad (confianza). |

| | | |
|---|---|---|
| CSC 13 | PROTECCIÓN DE LOS DATOS | Disponer de procesos y herramientas adecuadas para prevenir la fuga de información, mitigar los efectos cuando se ha producido un incidente de fuga de información, y asegurar la confidencialidad e integridad de la información sensible. |
| CSC 14 | ACCESO BASADO EN LA NECESIDAD DE CONOCER *(NEED TO KNOW)* | El acceso a los activos críticos debe realizarse de acuerdo a una definición formal de que personas, sistemas y aplicaciones tienen la necesidad y el derecho de acceso. Los procesos y herramientas utilizadas en el seguimiento, protección y corrección de estos accesos deben estar alineados con las definiciones. |
| CSC 15 | CONTROL DE ACCESO *WIRELESS* | Disponer de procesos y herramientas para garantizar una seguridad adecuada en las redes WiFi y en los sistemas clientes, incluyendo seguimiento y corrección de las medidas de seguridad. |
| CSC 16 | CONTROL Y MONITORIZACIÓN DE CUENTAS DE SISTEMA | Gestionar activamente el ciclo de vida de las cuentas de sistema y de aplicación (creación, uso, inactividad y borrado) para reducir su utilización por parte de un atacante. |
| CSC 17 | VERIFICACIÓN DE LAS HABILIDADES DE SEGURIDAD Y FORMACIÓN ADECUADA | Identificar los conocimientos específicos, habilidades y capacidades necesarias en la organización para la defensa de los activos críticos de la compañía, y desarrollar y evaluar un plan para identificar gaps y remediar con políticas, formación y programas de sensibilización. |
| CSC 18 | SEGURIDAD EN EL CICLO DE VIDA DE LAS APLICACIONES | Gestionar el ciclo de vida de todas las aplicaciones, tanto las desarrolladas internamente como las de proveedores para prevenir, detectar y corregir vulnerabilidades técnicas. |
| CSC 19 | GESTIÓN Y RESPUESTA A INCIDENTES | Proteger la información y la reputación de la organización desarrollando e implementando una infraestructura de respuesta a incidentes para detectar un ataque, contener el daño de forma efectiva, expulsar al atacante, y restaurar la integridad de los sistemas y la red. |
| CSC 20 | REALIZAR TEST DE PENETRACIÓN Y EJERCICIOS DE ATAQUE | Probar las defensas de la organización (tecnología, procesos y personas) mediante la simulación de un ataque, utilizando sus mismas acciones y objetivos. |

Fuente: NIST (02/14): Framework for improving Cyber-security.

**Para que el lector tenga una Buena y correcta interpretación de los controles, los mismos fueron transcriptos tal cual el paper de NIST (02/14): Framework for improving Cyber-security.**

**CONTROLES 1 Y 2**

"La revisión puede realizarse de dos formas:

· Verificar que existe una gestión de inventarios hardware y software, identificando listas blancas y negras y su actualización (al ser una aproximación de "ver que existe un control", podríamos llamarla, "de capa 2").

· El auditor interno escanea las redes internas utilizando herramientas automáticas (actúa como Red Team, según el control 20, es decir, comportándose como lo haría un atacante), hace una "verificación técnica", que podríamos llamar "de capa 1".

En el resto de controles también usaremos estas dos aproximaciones de revisión".

**CONTROLES 3 Y 4**

"Su revisión se puede enfocar, de forma complementaria a los controles 1 y 2, verificando si existe una política de bastionado de todos los dispositivos, aplicaciones y servicios, si esta política está alineada con buenas prácticas y si se dispone de un proceso de revisión de las vulnerabilidades que retroalimente la política de bastionado.

Otra aproximación es que el auditor escanee los dispositivos/aplicaciones utilizando herramientas automatizadas, actuando como Red Team".

**CONTROL 5**

"Este control nos lleva a que las cuentas de usuarios administradores de aplicaciones, dispositivos y sistemas operativos deben estar identificadas, su uso auditado, eliminando las que no se utilizan y cambiando las que están definidas por defecto. Adicionalmente, deben cumplir con la política de fortaleza de contraseñas.

La revisión de este control puede orientarse a verificar la existencia de una política de alta, baja y mantenimiento de usuarios administradores, y la fortaleza de la contraseña (debería formar parte de la política de bastionado), y las tareas que se desarrollan para comprobar su cumplimiento.

Por otro lado, también podemos solicitar el listado de usuarios definidos en los sistemas y los ficheros de contraseñas cifradas asociados, y comprobar que no disponen de las claves por defecto utilizando herramientas automáticas".

**CONTROL 6**

"Implica que todos los sistemas y aplicaciones deberían tener habilitadas las trazas de auditoría, incluyendo respuestas a desde dónde, quién, qué y cuándo, así como tener definidas acciones de alerta.

Debería existir una política asociada, un formato de log corporativo y una tarea de análisis de estos logs. En organizaciones con presupuesto y personal suficiente se suele disponer de un SIEM (Security Information and Event Management), sistema que permite disponer en tiempo real de alertas de seguridad.

La verificación pasa por analizar el contenido de los logs, y, si actuamos como Red Team, las actividades que realicemos, como escanear una red o conectarnos como usuario administrador desde un puesto no habitual, deberían reflejarse en los logs y generarse las alertas correspondientes".

**CONTROL 7**

"Nuevo en la versión 6.0, pasa por utilizar clientes de correo y navegadores actualizados y evitar que el usuario pueda añadir extensiones, así como cambiar su configuración. La configuración debe ser la más restrictiva posible para que el usuario pueda trabajar, deshabilitando los plugins innecesarios.

De forma complementaria, el control 8 habilita el análisis de malware en los equipos, y deben definirse medidas para evitar que el malware entre a través de la navegación del usuario o de la lectura de correo (IPS, antivirus de navegación y correo, bloqueo de URLs maliciosas, etc.)".

**CONTROL 8**

"El control 8 también recomienda agregar otras medidas contra el malware que deben estar recogidas en la política, como el bloqueo de USB y la monitorización continúa de los equipos.

Debe existir una política del uso seguro y de configuraciones autorizadas, y tareas de revisión automatizada de los equipos y servidores.

Otra posible verificación pasa por enviar un correo con contenido no autorizado a una cuenta interna, o navegar por una página dentro de una lista negra".

**CONTROL 9**

"Nos habla de limitar los servicios expuestos a las redes, y separar físicamente las máquinas que tienen esos servicios. Debe existir una política que defina que sólo los servicios y puertos necesarios para la organización estén habilitados, o restringidos a las redes/usuarios que realizan tareas asociadas. El resto debería estar deshabilitado/filtrado.
La aproximación para verificar este control pasa por realizar escaneos automáticos de las diferentes redes, para identificar puertos/servicios que deberían estar restringidos o deshabilitados.
Un auditor interno puede realizar esta tarea de forma puntual o verificar si existe un proceso continuo que lo realice".

**CONTROL 10**

"Nos pide que se hagan copias de seguridad de todos los datos críticos, así como que se verifique de forma periódica que estos se pueden recuperar en un tiempo asumible. Asimismo, los sistemas donde se guardan estas copias deben tener acceso restringido, tanto física como lógicamente.
Para probar este control, se pueden solicitar las políticas de back up y el resultado de las pruebas de recuperación".

**CONTROL 11**

"Se basa en definir una configuración segura para los dispositivos de comunicaciones (firewalls, routers, switches), junto con los procesos de gestión de cambio asociados. Este control es la implantación para estos dispositivos de los controles 3, 4 y 5: configuración base segura, revisión de vulnerabilidades y control del uso del administrador y, adicionalmente, control de cuentas por defecto (control 16).
El test de este control sería de la misma forma que los controles mencionados".

**CONTROL 12**

"En este control vemos que tenemos que tener una seguridad perimetral basada en aplicar filtros sobre las comunicaciones de nuestra organización hacia y desde fuera, así como desplegar sensores que detecten actividades sospechosas y alimenten a nuestro SIEM, tenemos que protegernos, pero también es importante detectar si están intentando entrar o, si ya lo han hecho, identificarlos".

“Por otro lado, tenemos que tener una DMZ, una zona donde los servicios expuestos a Internet estén separados de la red interna”.
“Si necesitamos acceder a la red interna desde fuera (teletrabajo), debemos implantar un segundo factor de autenticación”.
“El análisis de las reglas de FW nos permite evaluar este control. De igual forma que en controles anteriores, podemos hacer un escaneo de nuestro perímetro desde Internet para identificar puntos de entrada, servicios accesibles sin autenticación robusta y, testear qué alertas han generado nuestra actividad”.

**CONTROL 13**

“Este control confía en el cifrado de la información en reposo y en tránsito para garantizar la privacidad y prevenir una fuga”.

**CONTROL 14**

“El acceso a la información debe seguir el principio de “necesidad de conocer”. Un perfilado adecuado mitiga el riesgo, pero aun así debemos implantar otros controles, ya que un ataque puede obtener credenciales que tienen acceso a la información. Debemos emprender acciones complementarias, y algunos de los controles que hemos visto nos ayudan: limitar el uso de USB, monitorizar las conexiones o la separación entre redes”.
“La prueba del control tiene que ser empírica, intentar acceder a información a la que no tenemos acceso por perfil”.

**CONTROL 15**

“Nos dice que protejamos las redes wireless. Un inventario de todas las existentes, junto con revisiones periódicas por parte del área de seguridad de que no existen redes no autorizadas; la comprobación automática de sus vulnerabilidades y de la fortaleza de las contraseñas; y una limitación de las redes internas a las que se puede acceder; completan la revisión del control.
Adicionalmente, se deberían desplegar detectores de intrusos en estas redes para identificar dispositivos no autorizados”.

**CONTROL 16**

“Si el control 4 era qué hace el administrador, el 16 es si hay cuentas definidas en los sistemas que sean usuarios por defecto, usuarios que ya han abandonado la organización o si existen otras cuentas definidas en los sistemas”.

“Por otro lado, se deben establecer bloqueos de cuentas por accesos fallidos (este punto debería estar en la política de seguridad), limitando desde dónde se puede acceder y solicitando un doble factor para acceder a sistemas/ datos especialmente sensibles”.

Los accesos de terceros deben revisarse especialmente.

“Para probar este control, una opción es verificar que exista un proceso de revisión de usuarios. Otra opción es que Auditoría Interna lance herramientas automáticas para identificar cuentas obsoletas habilitadas”.

**CONTROL 17**

“Se basa en que cada puesto funcional tiene que tener una formación específica en seguridad”.

“Deben identificarse posibles carencias y formar a los empleados. Igualmente, la organización debería tener un programa de concienciación dirigido a todos los empleados, adecuado a las funciones que realizan”.

“Solicitar la formación recibida del personal de seguridad nos permite identificar las carencias”.

“Una forma de probar la efectividad es, una vez realizada la acción formativa/concientizadora, enviar un correo tipo phishing para ver la reacción del empleado y los pasos que realiza para denunciar el evento”.

**CONTROL 18**

“El ciclo de vida del software también necesita tener una capa de seguridad, como muestra el control 18. Tanto el desarrollo interno como la compra de software de terceros requieren de una capa de seguridad”.

“Las redes de desarrollo y producción deberían estar separadas.

Unas directrices de programación segura o plan de formación específica de desarrollo seguro, ayuda a evitar vulnerabilidades en las aplicaciones desarrolladas internamente. Si lo acompañamos de una revisión automática de código por parte de herramientas especializadas, limitamos las vulnerabilidades”.

“Una revisión final una vez integrado todo el desarrollo nos permite completar el ciclo. Esta última acción puede realizarla Auditoría Interna. Existen productos que filtran/limitan las vulnerabilidades más comunes, que también pueden desplegarse en producción.
Los productos de terceros deberían probarse antes de su implantación”.

**CONTROL 19**

“Se enfoca en la gestión de crisis. Es fundamental disponer de un plan de gestión y respuesta a incidentes que contemple procedimientos escritos, asignación de tareas y responsabilidades”.
“Estos planes deberían ser probados para verificar cómo está preparada la organización frente a un incidente de envergadura, y garantizar una gestión adecuada a la crisis”.

**CONTROL 20**

“Nos habla de realizar ciberejercicios. Los tipos de ataques no paran de crecer. Aparecen nuevas técnicas de las que nos tenemos que defender”.
“Una forma de probar si tenemos las defensas adecuadas es comportarnos como un posible atacante utilizando técnicas similares”.
“La capa 2 puede realizar esta tarea. Auditoría Interna revisaría las situaciones identificadas y las acciones correctoras”.
“Auditoría Interna también puede realizar la tarea (prueba todos los controles), o contratar los servicios de un externo”.

## 3.3 Interpretación y análisis sobre el Trabajo de Campo realizado

Del trabajo de campo realizado a dos profesionales relacionados directamente en el área de Auditoria Interna en sus respectivas organizaciones, y siendo estas de rubros y actividades totalmente distintas. En ambos casos pudimos observar que la pandemia produjo las mismas dificultades a la hora de aumentar los controles para la detección y prevención de los delitos informáticos.

La palabra Ciberseguridad no le resulta distante a ninguno de los profesionales entrevistados y ambos coinciden que el trabajo remoto y la falta de feedback con los clientes encendió las alarmas aún más a la hora de tomar recaudos en operaciones financieras.

Otro punto importante que pudimos desarrollar a través de la bibliografía consultada y que ambos profesionales hacen hincapié, es que el problema del ciberdelito no le corresponde solamente al área de informática, sino que toda la organización debe encontrarse involucrada con el problema, comenzando con la gerencia.

Cuando nos referimos al trabajo remoto, ambos toman como una ventaja la reducción de costos en movilidad y tiempo, pero a la vez se hace una erogación importante de dinero en nuevas tecnologías para poder brindar un servicio de calidad a sus clientes, dado que millones de personas se sumaron al uso de las conexiones de red y en muchos casos se torna ineficiente el manejo de información en la nube.

Si bien podemos encontrar plasmado en las entrevistas lo que algunos autores a través de sus libros nos describen con mucha claridad, la experiencia enriquecedora que con lleva tener la información de fuente primaria, nos deja una enseñanza para nuestra vida profesional muy valiosa.

## CONCLUSION:

El presente trabajo tiene como objetivo brindar al lector aquellas herramientas con las que cuenta la Auditoria Interna en las organizaciones para prevenir y detectar aquellos ataques informáticos que en esta época de Pandemia se fueron incrementando, dado que la situación sufrida a nivel mundial hizo de estos delitos un escenario propicio para llevarlos a cabo.

El primer inconveniente que las organizaciones y el mundo en general tuvo que afrontar es que no estaba preparado para la llegada del Covid 19 y si hablamos de Ciberdelito en Argentina en estos tiempos, una de las cosas que primero se percibe es la poca información disponible sobre las leyes a nivel latinoamericano. Por lo tanto, en muchos casos los usuarios tienen que realizar un trabajo casi de investigación para conocer qué leyes existen y qué garantizan, ya que la información no esta tan a mano cómo se esperaría.

Si bien como mencionamos anteriormente contamos con un marco legal para estos casos, la principal herramienta utilizada por las organizaciones es la Ciberseguridad, de hecho en las Universidades de la Republica Argentina hoy se dicta la Carrera de Tecnicatura en Ciberseguridad y algunas universidades dictan la Diplomatura en Ciberseguridad.

Desde el comienzo de la pandemia, los ciberataques aumentan de manera exponencial a escala mundial. Según el estudio anual de delitos en internet de 2020 realizado por el departamento de cibercrimen del FBI, las denuncias por delitos informáticos se duplicaron respecto a 2019. En el caso de la Argentina, hubo más de 900 millones de intentos de ciberataques el año pasado y solo en el último trimestre del año pasado hubo 550 millones, de acuerdo a datos de la multinacional estadounidense Fortinet.

Es por todo esto, que la Auditoria Interna tiene una responsabilidad importante a la hora de acompañar a la gerencia en la prevención del ciberdelito, no solo desde el asesoramiento continuo para la implementación de nuevas tecnologías, sino contar con el personal idóneo para mitigar el fraude informatico que continuamente evoluciona de diferentes formas(**Fingerprinting, APT (Amenaza Persistente Avanzada), Phishing o Vishing, o programas o virus)** que afectan principalmente a entidades bancarias o Gobiernos.

## BIBLIOGRAFIA:

### LIBROS


- Carlos Alberto Slosse (2013), Auditoria Tercera Edición
- Nelson, L. (2020). “Modelo para gestionar el riesgo de fraude corporativo durante una Pandemia”, de Instituto de Auditores Internos de Argentina
- Código Penal de la Nación Argentina.
- LEY 26.388 de Ley de Delitos Informáticos.

- LEY 27.411. Aprobación del Convenio sobre Ciberdelito (Convenio de Budapest sobre Ciberdelito)

- NIST (02/14): Framework for improving Cyber-security.


**PAGINAS WEB**


- https://nic.ar/es/enterate/novedades/que-es-ciberseguridad
  Consulta: 10 de Marzo 2020

- http://www.fatf-gafi.org/pages/aboutus/
  Consulta: 4 de mayo 2020

- https://capacitacion.inap.gob.ar/actividad/introduccion-al-ciberdelito/
  Consulta: 18 de Octubre 2020

- https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito
  Consultado: 5 de Noviembre 2020

- http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf
  Consultado: 6 de Marzo 2021

- http://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm
  Consultado: 27 de Marzo 2021

- https://www.welivesecurity.com/la-es/2017/02/10/leyes-argentinas-delitos-informaticos/
  Consultado: 8 de abril 2021

- https://nic.ar/es/enterate/novedades/que-es-convenio-budapest
  Consultado: 26 de abril 2021

- http://www.saij.gob.ar/27411-nacional-aprobacion-convenio-sobre-ciberdelito-consejo-europa
  Consultado: 26 de abril 2021

- https://www.infotechnology.com/actualidad/estudiar-ciberseguridad-en-argentina-ahora-se-puede-hacer-gratis/

Consultado: 10 de septiembre 2021

# ANEXOS:

## ENTREVISTA 1

Nombre: NICOLAS PATRICIO ROCCA

Profesión: CONTADOR PUBLICO

Empresa: MAKINGPROGRESS SA

Cargo: SOCIO

1. ¿Cómo las funciones de auditoría interna han abordado el riesgo de fraude como resultado de COVID-19?

**Los riesgos derivados de ciberseguridad como fugas de información, fraudes, castigan económicamente a las organizaciones, o pueden llegar a parar la operativa o prestación del servicio de las compañías, dicho esto hay que extremar las medidas en materia de ciberseguridad y establecer todos los controles necesarios para poder disminuir los riesgos en las organizaciones.**

2. ¿Cómo ha cambiado su plan de auditoría como resultado de COVID-19?

**Teniendo en cuenta las circunstancias, se debe tener un rol más de consultor que de aseguramiento.**

**Hoy más que nunca debe estar de lado de la alta gerencia para apoyar en la identificación de nuevos riesgos y en la asesoría y soluciones de negocio que permitan palear esta crisis en el corto, mediano y largo plazo. Algunas de estas acciones que debe tomar auditoría interna incluyen lo siguiente:**

**Enfocarse en asesorar a la gerencia en la ejecución del plan de continuidad de negocio y manejo de crisis. Muy probablemente, el plan de continuidad de negocio**

**no incluía respuestas a este tipo de situaciones, sin embargo, el auditor interno en su rol de consultor puede apoyar a establecer medidas para mitigar riesgos emergentes que surjan de esta crisis.**

3. ¿Cómo ha cambiado la estructura de los equipos de auditoría interna como resultado del COVID-19?

**Dada la situación generada por el COVID-19, algunos grupos se redujeron, disminuyendo la cantidad de personal, pero en líneas generales se mantuvieron los equipos, sin incorporar nuevos miembros.**

**Los cambios radican en más control en ciberseguridad debido al aumento del riesgo derivado del trabajo remoto.**

4. ¿Cuáles son las principales limitaciones con las que se encontró el sector de AI al comienzo de la pandemia?

**Las limitaciones a la observación, la disponibilidad del auditado, las dificultades en el acceso de las evidencias o para hacer las pruebas necesarias han sido grandes restricciones a la hora de ejecutar los procesos.**

**Esto obliga al auditor interno a tener una visión global, analizar riesgos constantemente, a conocer más el proceso.**

5. Ventajas y Desventajas del trabajo remoto ante periodos de auditoria interna

**Ventajas:**

## Eficiencia en tiempo y costos

**Los auditores pueden recaudar información subida a una "nube" sin necesidad de acudir a las empresas.**
**Esto implica reducir costos de dinero y tiempo para viajes que podrían evitarse, también se utilizan técnicas como realizar entrevistas o formular observaciones, esto se puede realizar a través de video llamadas.**

## Aprovechar las funcionalidades de la tecnología

**Las organizaciones hacen inversiones en tecnología que implican grandes erogaciones de dinero.**
**El trabajo remoto, motivo a explotar al máximo dichas inversiones.**

**Desventajas:**

## Los requerimientos tecnológicos pueden ser un problema para Pymes.

**Conexiones de red deficientes, ausencia de almacenamiento en la nube, pueden dificultar la tarea. Cortes en la conexión o dificultad para el acceso a la información.**

## Pérdida de día a día

**La pérdida de las reuniones de grupo, o el feedback del "día a día".**

6. ¿Cuáles son las acciones tomadas por el sector de Auditoria Interna para ajustar las posibles estrategias de fraude ante el avance del Ciberdelito en pandemia?

**Las funciones de AI han abordado el riesgo enfocándose en diferentes tratamientos para mitigar ese riesgo, ya sea desde el cuidado con correos electrónicos sospechosos, dispositivos móviles, redes Wifi, redes sociales.**

**El uso adecuado de los mismos, conforme a las políticas de seguridad de la compañía provee una garantía que minimiza el riesgo, como así también desarrollar e implementar las políticas generales (ciberseguridad) y facilitar el desarrollo e implantación del marco general de riesgos y controles o establecer las metodologías para evaluar y monitorizar el proceso.**

7. ¿Qué medidas considera preventivas tomar para limitar comportamientos fraudulentos?

**La decisión de medidas preventivas es responsabilidad de la gerencia, la auditoría interna tiene a cargo la evaluación de los procedimientos y medidas preventivas que tienden a detectar errores y fraudes.**

**La auditoría Interna debe ser eficaz para evitar dichos errores y/o fraudes.**

**Un buen equipo de auditoría interna puede resultar de gran ayuda para llevar a cabo aspectos de la función de vigilancia, permitiendo que la organización sea monitoreada con regularidad y se dicten políticas y procedimientos que permitan enfrentar las nuevas situaciones de fraude que surgen.**

**El conocimiento que obtenga la auditoría interna del entorno y actividades de la empresa puede servirles para identificar factores que sugieran que se ha cometido un fraude.**

**Las medidas preventiva rondan en torno a:**

**- Se respete la segregación de funciones**

**- Hacer recomendaciones para el ente y así mejorar los controles para desalentar y prevenir el fraude.**

**- Generar canales de comunicación proporcionan a la dirección información adecuada y confiable.**

8. ¿Cómo auditoria interna puede entregar revisiones de alta calidad a través del trabajo remoto?

**Se debe considerar un aumento del uso de las capacidades tecnológicas disponibles, para poder realizar reuniones virtuales con eficiencia, como así también aumentar los recursos a fin de incluir tareas adicionales para fortalecer el trabajo remoto.**

## ENTREVISTA 2

Nombre: PATRICIA RUSSO

Profesión: CONTADOR PUBLICO

Empresa: SERRA RICCO SA

1. ¿Cuáles son las principales limitaciones con las que se encontró el sector de AI al comienzo de la pandemia?

**La pandemia exigió a las organizaciones replantear sus procesos de negocios, asegurando que las operaciones fluyan a como dé lugar: las restricciones de movilidad y la prioridad de atender los temas sanitarios demanda la toma de decisiones de emergencia, que eventualmente, exigen simplificar su aprobación y ejecución.**

**Las adaptaciones tienen las siguientes características:**

- **Se ejecutan para atender una necesidad específica y eventualmente coyuntural.**
- **Se construyen con lo que tengo y no con lo que necesito.**
- **Se diseñan en un escenario en donde todas las partes relacionadas están cambiando.**
- **Se plantean considerando una nueva normalidad que es aún desconocida.**

2. Ventajas y Desventajas del trabajo remoto ante periodos de auditoria interna

**Ventajas:**

- **Reducción de los costos de desplazamiento**
- **Amplio grupo de auditores disponibles (NY, Tennessee, Bs As)**
- **Uso amplio de especialistas**
- **El uso mejorado de la tecnología disponible fortalece la documentación y la presentación de informes**
- **La carga de auditoría para las operaciones de las instalaciones se reduce**
- **Mejora de la organización y conformación de la documentación necesaria**

**Desventajas:**

- **Las observaciones de primera mano no se pueden sustituir (lenguaje corporal, olores)**
- **Dificultad para crear relaciones con los auditados (se pierden oportunidades de sugerencias, consejos y observaciones)**

- **La falta de interacción en persona abre otras oportunidades de fraude. Aumenta la posibilidad de presentar documentación adulterada y omitir información pertinente**

3. ¿Cuáles son las acciones tomadas por el sector de Auditoria Interna para ajustar las posibles estrategias de fraude ante el avance del Ciberdelito en pandemia?

**Además de los riesgos de fraude laboral está el delito cibernético, el cual plantea un gran desafío. A medida que el Covid 19 (pandemia) se extiende por el mundo y millones de personas han comenzado a trabajar a distancia, el riesgo de ser víctimas de una amenaza cibernética aumentó considerablemente.**

**La mitigación de las amenazas cibernéticas debería ser un esfuerzo de toda la empresa y no solo del sector informático**

- **Tener cuidado cuando hace clic en enlaces desconocidos**
- **Pensar 2 veces antes de proporcionar datos financieros corporativos e información personal**
- **Tener cuidado de no descargar un archivo sin verificarlo**

4. ¿Qué medidas considera preventivas tomar para limitar comportamientos fraudulentos?

**Ante todo sepamos algunos conceptos que originan el fraude**

- **Trabajo remoto (menor control de procesos)**
- **Presiones del entorno (reducción de sueldos, despidos)**
- **Racionalización de los motivos que llevan al fraude**

**De forma tal que para poder reducir el comportamiento fraudulento, se requiere de esfuerzo en conjunto, de procesos adecuados para la gestión de fraude y contar con personal especializado en prevención, detección e investigación de prácticas corruptas dentro de la empresa.**

**Frente al Covid 19 las empresas están gestionando los impactos para resistir frente a este período de incertidumbre y aparecen nuevos focos de atención con la**

**gestión de la crisis: fuerza laboral, continuidad de negocios, reducción de costos, entre otros tantos.**

**Es por ello que la AI está en una posición única para desempeñar un papel clave en respuesta a la crisis del Covid 19, partiendo de un correcto conocimiento organizacional y con un conjunto de habilidades muy relevantes.**

**A medida que la pandemia continúa, la AI considera nuevas ideas y consideraciones, es por ello que la AI debe ser práctica y pragmática.**

**Rol de AI: Adoptar un enfoque de gestión ágil del portfolio. Adopte una priorización a corto plazo (revisiones/oct periódicas para reflejar el ritmo cambiante de las necesidades de riesgo y aseguramiento).**

**Adoptar y aumentar el uso de tecnología (zoom-skype) para reuniones.**

5. ¿Cómo auditoria interna puede entregar revisiones de alta calidad a través del trabajo remoto?

**La clase para realizar con éxito auditoria en remoto:**

**1- Identificación de interlocutores: es necesario contar con interlocutores que dediquen un tiempo a la elaboración de la agenda, tanto auditor como auditado.**

**2- Análisis de tecnología disponible: los interlocutores deberán evaluar la viabilidad del proyecto en función de las herramientas tecnológicas a las que ambas partes tienen acceso.**

**3- Selección de herramientas: garantiza la viabilidad, es el momento de definir con que instrumentos se contaran tanto para compartir archivos, mantener reuniones y así garantizar el acceso y visualización de información.**

**4- Documentación necesaria: una vez acordadas las herramientas a utilizar, es necesaria comunicar nuevamente la información documentada que se necesitara. Para ello se informó de los documentos que son necesarios revisar para garantizar que el equipo auditor pueda constatar la implantación del sistema de gestión, su seguimiento y mejoras continuas.**

**5- Intercambio de archivos: esta información puede ser alojada en espacios virtuales compartidos donde las partes implicadas tengan acceso, ya sea por correo electrónico, las nubes, etc.**

**6- Gestión de horarios: es de gran importancia estimar el tiempo de dedicación que lleva auditar cada proceso. De esta manera se podrá convocar a los interlocutores a unas horas determinadas realizando bloques de tiempo. Se deberá determinar los tiempos de descanso que se necesitan (almuerzo)**

**7- Pruebas previas: para garantizar el éxito de la auditoría será importante realizar pruebas antes de su comienzo y asegurar que todos los interlocutores tienen acceso tanto a las herramientas documentadas como aquellas que permitirán las reuniones online.**

**8- Convocatoria de reunión por procesos: una vez cumplidos los asuntos anteriores se procederá a convocar las reuniones con cada interlocutor de cada proceso, a través de los medios seleccionados. En este sentido se realizarán tanto convocatorias como procesos lo requerirán. También se deberá contemplar no duplicar personal auditado.**

**9- Clima laboral: un aspecto importante es crear un clima laboral. De esa manera se podrá elevar el nivel de concentración, se dedicará tiempo a seleccionar el lugar de trabajo con el fin de garantizar que sea el más tranquilo posible. Por otro lado y dado que la interlocución se hace a través de una pantalla o audio, es conveniente mantener signos de interlocución de manera constante. Tratar de ausentarse lo menos posible (café, agua).**

**10- Contar con los suministros: es posible que durante la auditoría se produzcan imprevistos tales como falta de acceso a las redes. En estos casos la capacidad de reacción no diferirá en gran medida de la auditoría in situ, pudiendo re planificar las entrevistas.**