Revista Finanzas y Negocios
ISSN 2710-7809
Vol.4, No.1: 8-31
Enero – Abril 2024
Panamá

El papel del control interno dentro de la ciberseguridad basado en el Modelo COSO - ERM

The role of internal control within cybersecurity based on the COSO Model - ERM

Rogelio Bouche[1], Ramses Owens[2]

[1]Profesor Investigador. Universidad UNIDOS. Ciudad de Panamá. Panamá.
https://orcid.org/0000-0002-4015-3218 rbouche@unidos.edu.pa

[2]Licenciatura en contabilidad. Universidad UNIDOS. Ciudad de Panamá. Panamá.
https://orcid.org/0009-0003-3163-8269 rowens@unidos.edu.pa

Fecha de Recepción: 01/10/2023 *Fecha de Aceptación: 8/12/2023*

Resumen

Con esta investigación hemos querido estudiar cuál es el papel del Control Interno, con relación a la mitigación del riesgo cibernético, denominado como un riesgo emergente producto de la sociedad hiperconectada de hoy día. Todo emprendimiento o actividad empresarial actualmente requiere de dos cosas muy relevantes para el éxito futuro de su operación, estos elementos son: El control interno y utilización de herramientas tecnológicas para posicionarse en el ciberespacio, que es el sitio donde se encuentran sus clientes. Basado en esta premisa es obligatorio tener posicionamiento en las redes sociales o la llamada "huella digital" en conjunto con procesos de control para todas las actividades de negocio, teniendo en cuenta que dichos controles deben ser diseñados para ayudar a los objetivos empresariales sin dificultar la actividad económica del negocio. El artículo aborda el tema de la ciberseguridad, que es una preocupación constante para las organizaciones modernas que dependen de la información digital. El enfoque principal del artículo es el control interno y la gestión de riesgos empresariales del COSO ERM, que es un conjunto de políticas, procedimientos y herramientas para hacer frente a los riesgos de seguridad cibernética. El artículo explica que la ciberseguridad es la práctica de proteger los sistemas tecnológicos y la información confidencial de los ataques digitales. También se discute la evolución del COSO ERM desde su introducción en 2004 hasta la versión actual de 2017, que aborda los peligros e inseguridades cibernéticas en las organizaciones modernas. Al finalizar nuestra investigación logramos concluir que debemos cambiar el enfoque hacia el ciber-riesgo y apoyarnos en modelos eficientes para su mitigación.

Palabras clave: Control Interno, Control, Ciberataque, Ciberseguridad.

Abstract

With this research we wanted to study the role of Internal Control, in relation to the mitigation of cyber risk, called an emerging risk product of today's hyperconnected society. Every venture or business activity currently requires two very relevant things for the future success of your operation, these elements are: Internal control and use of technological tools to position yourself in cyberspace, which is the place where your customers are. Based on this premise, it is mandatory to have positioning in social networks or the so-called "digital footprint" in conjunction with control processes for all business activities, taking into account that said controls must be designed to help business objectives without hindering the economic activity of the business. The article addresses the topic of cybersecurity, which is a constant concern for modern organizations that depend on digital information. The main focus of the article is the internal control and enterprise risk management of COSO ERM, which is a set of policies, procedures, and tools to address cybersecurity risks. The article explains that cybersecurity is the practice of protecting technological systems and confidential information from digital attacks. The evolution of COSO ERM from its introduction in 2004 to the current 2017 version, which addresses cyber dangers and insecurities in modern organizations, is also discussed. At the end of our investigation, we were able to conclude that we must change the focus towards cyber-risk and rely on efficient models for its mitigation.

Key words: Internal Control, Control, Cyberattack, Cybersecurity.

Introducción

El trabajo que nos ha ocupado, denominado ***"el papel del control interno dentro de la ciberseguridad basado en el Modelo COSO - ERM"***, es tremendamente abarcador, porque trata sobre el vasto tema de la información digital, es decir, un componente impostergable, ineludible y consubstancial de toda organización moderna. El presente trabajo intentará cubrir los elementos esenciales del control interno, haciendo énfasis principalmente en la gestión de riesgos empresariales del COSO ERM II (compendiado al 2017), más que en el Sistema de Control Interno, quizás ya un poco obsoleto de COSO I (esquematizado al 2013), como un conjunto de políticas, procedimientos y herramientas para hacerle frente, a nivel razonable, al riesgo siempre inminente de la seguridad cibernética.

Tengamos presente que el término ciberseguridad, es una mixtura entre "cibernética" y "seguridad". **Cibernética**, de forma simplista, es la ciencia de los sistemas de control y comunicación basados en retroalimentación, respaldados o impulsados por la computación, con los sistemas electrónicos y mecánicos que en ellos existe. Es decir, que cibernética es el conjunto de todas las conexiones, vía computacional o de informática, de comunicación artificial.

Como sustantivo, la cibernética es una ciencia. La palabra viene del vocablo griego "kybernetes", que se refiere al arte de gobernar una embarcación. Como adjetivo, es lo creado o gobernado mediante computadora. En el texto del trabajo,

ahondaremos un poco sobre los derivados del concepto de “cibernética”.

A su vez, la segunda palabra de “ciberseguridad”, es **“seguridad”**, que alude a la ausencia de peligro o sensación de confianza de que no se provocará daño físico o material que pudiese impactar a la organización para cumplir con sus objetivos.

Una vez hemos descompuesto los vocablos del término “ciberseguridad” en los párrafos precedentes, podemos entonces decir que, “ciberseguridad”, en un significado elemental y asequible, que traemos citado de la organización transnacional IBM, es “la práctica de proteger los importantes sistemas tecnológicos y la información confidencial, de los ataques digitales”.

Escrito de la manera más simple y sencilla, la ciberseguridad es la “seguridad informática”.

El presente trabajo se denomina “el papel del control interno dentro de la ciberseguridad basado en el modelo COSO - ERM”, es decir, la ciberseguridad en su necesidad de que haya control interno organizacional para protegerla. Es por ello, que resulta imperioso que repitamos, a manera de introducción del trabajo, la significación que se le ha dado al término “Control Interno” según COSO I y COSO II ERM, cual es ***“un proceso llevado a cabo por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos de eficacia y eficiencia en las organizaciones”.***

No podemos soslayar el hecho de que la Gestión de Riesgo Empresarial COSO II (**ERM**, por sus siglas en inglés) ha ido evolucionando en el tiempo, desde el 2004 hasta el 2017. Como bien se puede mencionar que, la Gerencia de Control Tradicional ha sido cambiada por una Gerencia de Riesgos, en virtud de la introducción del e-business. El e-business alude, para los efectos del presente trabajo, al mundo cibernético de nuestras organizaciones vanguardistas contemporáneas. El perfil de los riesgos incorpora actualmente los peligros e inseguridades electrónicas, computacionales y cibernéticas.

Desarrollo

Antes de aterrizar en el tema de la ciberseguridad y la necesidad de control interno para su salvaguarda, dentro de la gran diversidad de riesgos contemporáneos, hemos consultado una gran variedad de bibliografía española y otras nacionalidades, e infografías sobre el tema de ciberseguridad y sus líneas de defensa.

Sabemos que la ciberseguridad se refiere a las tecnologías, los procesos y las

prácticas concebidas a fin de protegerse del acceso no autorizado a los activos de información presentes en una organización. En ese sentido, el término "ciberseguridad", como explicábamos en la introducción, se compone de dos palabras: "cibernética y seguridad". En ese mismo orden de ideas, existen otros términos de uso común, los cuales, deseamos traer como antecedentes al presente trabajo, y que se relacionan con la expresión genérica "ciberseguridad":

Ciberdelincuencia: Se refiere a cualquier actividad ilegal vía internet, llevada a cabo mediante el uso de la tecnología. El ciberdelincuente es aquel que, por medio de actos ilegítimos y antijurídicos, provoca daños y/o pérdidas materiales, intangibles, reputacionales y/o dinerarias a sus víctimas;

Ciber-riesgos: Es cuando se produce una situación de vulnerabilidad en una empresa debido al acceso ilegal a datos o a fallos de seguridad de los sistemas informáticos, lo cual lleva a la idea de que es muy complicado proteger por completo una empresa y aislarla de posibles ataques cibernéticos;

Cibercrimen: Es una actividad delictiva que se dirige a una computadora, una red informática o a un dispositivo en red, o bien que utiliza uno de estos elementos, entendiéndose que la mayor parte del cibercrimen está cometido por cibercriminales o hackers que desean ganar dinero.

Control interno dentro de la ciberseguridad:

El Control Interno en COSO ERM - 2017

El presente trabajo de investigación nos advierte que debemos enfocarnos en el control interno, como ingrediente de la ciberseguridad. Es por esta razón, que creemos conveniente brevemente esclarecer que el desarrollo de la materia lo hacemos basándonos en el enfoque de "riesgo", es decir, asentados en los componentes y principios de COSO ERM - 2017, con sus nuevas denominaciones, a saber: Gobierno y Cultura; Estrategia y Definición de Objetivos; Desempeño; Análisis y Revisión; y la Información, Comunicación y Presentación de Informes, que como sabemos, contiene 20 principios.

Entre todos los avances en materia de Gestión de Riesgos Empresariales, especial interés nos ha suministrado COSO ERM - 2017 en darle valor a la inversión capitalista de la empresa; y atención en sus objetivos de actualización. COSO ERM - 2017 dio primordial relevancia a las decisiones estratégicas, dando énfasis en la evaluación de desempeños y el control o gestión de calidad, en actitud propositiva y

proactiva, adelantándose a los hechos y evitando el encuentro con sorpresas.

Implicación de los avances de COSO ERM - 2017 en la gestión de riesgos en materia de ciberseguridad. Evaluación de Riesgos de Ciberseguridad en tres líneas de defensa.

Un tema que no podíamos dejar por fuera es el de las implicaciones que ha tenido COSO ERM - 2017 en el desarrollo del tema de ciberseguridad.

Nos resulta imperioso citar al Profesor Fernando Román (PWC, México), de sus interesantes exposiciones realizadas en sendos audiovisuales, los cuales se reseñan en la sección de bibliografía / infografía. El Profesor Román, hace hincapié en que los avances en la priorización de la ciberseguridad, dentro de COSO-2017, se centran en el enfoque contenido en el componente "Gobierno y Cultura", basado en el hecho de que ahora hay nítidas responsabilidades en ese sentido. Con COSO-2017, ahora están más claras y definidas las responsabilidades, y la necesidad de que haya conocimientos sobre las amenazas de la ciberseguridad, lo cual es un progreso que implica mucho. En COSO ERM - 2017, se enmarca como "estrategia organizacional", que haya capacitación sobre ciberseguridad en todos los niveles de la entidad, sobre todo en "primera línea" de defensa, pero sin que adolezca en la "segunda línea de defensa". Para COSO II (ERM 2017), es vital que haya esta especial gestión de riesgo, puntualizando en la ciberseguridad, y que sea en actividades diarias, en protección en tiempo y en forma.

Como bien matiza el profesional de PWC-México, antes de COSO ERM 2017, se consideraba que la "seguridad de la información" era un mundo distinto al diario vivir organizacional. Hoy en día, se considera que el riesgo inherente de ciberseguridad está en constante evolución, razón por la que debe haber creciente interconectividad, que sea monitoreada constantemente, con sus respectivos controles, de tal forma que esas amenazas no exploten vulnerabilidades. Todo esto, dentro de lapsos que mitiguen nuevos riesgos, para poner en práctica acciones de tratamiento adecuadas. Fernando Román pone especial atención a la relevante comunicación que debe haber entre la primera y segunda línea de defensa frente a los riesgos de seguridad de la información. Román aterriza en el sentido de que ***la principal implicación de los avances de COSO ERM 2017, es que la gestión de riesgos en materia de la ciber-seguridad, ahora forma parte de las "decisiones estratégicas de los negocios"***. Para mejor desarrollar esta respuesta, sobre todo

en el presente trabajo final del curso, investigué adicionalmente en libros de la Biblioteca E-Libro de UNESCPA, y en varias infografías, sobre las líneas de defensa frente a la ciberseguridad.

Visitamos estos libros de edición española: “Ciberseguridad”, de Gayoso Martínez, 2020, Editorial del CSIC Consejo Superior de Investigaciones Científicas; “Normativa de Ciberseguridad”, de Nuria Gómez, 2021, de RA-MA Editorial; “Gestión de Incidentes de Seguridad”, de Maite Moreno, 2022, también de RA-MA Editorial; “Estrategias de Marketing digital en un entorno ciberseguro”, de Natalia Grech, también de RA-MA Editorial; y “Ciberseguridad: Un nuevo Reto para el Estado y los Gobiernos Locales”, de Dolors Canals, 2021, de Editorial Wolters Kluwer. En adición a estos libros, especial atención aposté a varias infografías sobre las tres (3) líneas de defensa, para destacar mejor la relevancia que tiene la administración estratégica de la seguridad de la información. Descargamos el enlace del Institute of Internal Auditors (IIA), sobre “Las Tres Líneas de Defensa para una Efectiva Gestión de Riesgos y Control” (link: https://shre.ink/kvKF).

También estuvimos dentro de Global Suites Solutions, en un interesante escrito denominado “Automatización del Modelo de las 3 líneas de defensa” (link: https://shre.ink/kvKV). Igualmente, visitamos a Miranda-Partners dentro de su página: https://shre.ink/kvBS . No quisimos dejar por fuera la sección de COSO sobre ciberseguridad de B2B México en: https://shre.ink/kvBg .

Nos adentramos igualmente al estudio del trabajo de la Fundación Latinoamericana de Auditores Internos (FLAI), como Guías Complementarias GTAG, que contiene también material sobre la “Gestión de Riesgo Empresarial”. En aras de explicar el “sistema control interno” dentro de la ciberseguridad, hemos querido también en este trabajo final hacer un resumen de lo investigado en estas varias infografías, y que son parte de las implicaciones de los avances en ciberseguridad. De esta manera, debemos destacar que el riesgo, y su control interno que se opone a ese riesgo, debe llevarse a cabo o practicarse en todos los niveles de la organización. Los principales actores que participan directamente en las operaciones de control interno basado en riesgos de Seguridad Cibernética son: ***La Primera Línea de Defensa***: La Alta Dirección o el Consejo de Administración, es decir, la propietaria de los riesgos en primera instancia, con la responsabilidad de tomar decisiones estratégicas en cuantificación cualitativa y cuantitativa.

La Segunda Línea de Defensa: Es decir, por los departamentos de Seguridad

de Sistemas, Cumplimiento Normativo de Tecnología de la Información (TI), Asesoría Jurídica, Cumplimiento, Debida Diligencia, entre otros, los cuales deben desarrollar e implementar la infraestructura y componentes de TI, las áreas de computación de laptops, aparatos móviles y hojas de cálculo; las aplicaciones de TI subcontratadas en la nube; y cómo se administra la función de tecnología de toda la organización.

Y ***La Tercera Línea de Defensa***: Recae sobre la Auditoría Interna, que debe revisar y evaluar, de forma independiente, realizando investigaciones con el personal, procedimientos analíticos, observación de procesos e inspección de documentos.

En todos los supuestos explicados, deben estar alineados los riesgos de la empresa, con sus objetivos, para establecer estrategias, tal como enfatiza COSO ERM 2017. Las tres líneas de defensa deben también interactuar con todo el personal ejecutivo u operacional, vía seminarios o talleres.

Fraudes cibernéticos. Un tema de ciberseguridad. Controles para neutralizarlos.

No hemos querido desplegar el trabajo, sin hacer un breve recuento de los diferentes fraudes que enfrentamos como posibles riesgos cibernéticos y controles de seguridad de la Tecnología de la Información:

a. **Malware**, que son softwares dañinos.
b. **Phishing**, que son suplantaciones de identidad.
c. **Virus.** Insertar un malware que se adhiere a otros programas y se auto replica para causar daño.
d. **Hacking (hackeo).** Extracción parcial o masiva de información.
e. **Correo basura o spam.** Descargar archivos que realiza un despliegue de programas hostiles.
f. **Smishing.** Mensajes SMS para obtener informaciones de forma fraudulenta.
g. **Pharming.** Redirigir a páginas falsas de internet.
h. **Ramsonware.** En informática, es un tipo de ***malware*** o código malicioso que impide la utilización de los equipos o sistemas que infecta, tomando el ciberdelincuente el control del equipo o sistema infectado y lo 'secuestra' de varias maneras, cifrando la información, bloqueando pantallas, etc., lo cual se presta mucho hoy en día para extorsiones, conforme se evidencia en sinnúmero de reportajes noticiosos.
i. **Denegación de Servicio (DOS)**, lo cual es atacar o saturar el tráfico hacia un servidor, para lo cual se utiliza mucho, para contrarrestarlo, el estándar ISO 27001.

j. **Confidencialidad.** Consiste en hacer llegar informaciones a personas no autorizadas.

k. **Integridad**. Modificar información a través de ***virus***.

l. **Disponibilidad.** Acceso a personas no autorizadas.

Controles para neutralizarlos:

(i) **Controles físicos para prevenir riesgos cibernéticos.** Cámaras de Circuito Cerrado, sistemas de alarmas térmicas o de movimiento, guardias de seguridad, identificación de fotos, puertas de acero con seguros tecnológicos de acceso con biométrica (huellas dactilares, voz, rostro, iris, y demás).

(ii) **Controles técnicos.** Encriptación, tarjetas inteligentes, autenticación a nivel de la red, listas de control de acceso, y softwares de auditoría de integridad de archivos.

(iii) **Controles administrativos.** Entrenamiento, plan de recuperación, preparación de desastres cibernéticos, estrategias de selección de personal idóneo y ético, más el registro adecuado del personal.

Transformaciones para implantar elementos de ciberseguridad de acuerdo con los cambios de COSO- ERM

Como también manifestamos en anteriores trabajos, COSO ERM - 2017 ha evolucionado lo suficiente, como para colocar el riesgo de seguridad de la información y cibernética en un plano de muy alta gerencia, es decir, en el nivel donde se toman las decisiones estratégicas, en virtud de que, en la actualidad, buena parte de las comunicaciones y desarrollos empresariales se ponen en práctica haciendo uso de las tecnologías de la información, las cuales enfrentan los riesgos cibernéticos. Así, a mi juicio, las empresas deben introducir, en materia de ciberseguridad, al menos, los siguientes cambios, con lo cual concuerdo con las herramientas de infografía investigadas:

a. Orientación hacia la ciberseguridad. Las tres líneas de defensa (alta gerencia, departamentos de seguridad de la información y auditoría interna, deben coordinarse para la realización de talleres (foros colaborativos, reunión

de líderes con consultores externos, y demás), en los que participe suficiente personal que represente buena parte de la organización. De relevante importancia, es la concientización del personal en materia del peligro actual del desafío de los virus cibernéticos, y cómo enfrentar este flagelo.

b. ***Poner en funcionamiento los marcos de normas ISO***, como pueden ser: ISO 27032, ISO 27014, ISO 27000, ISO 31000 (la cual es ampliamente utilizada) y otras.

c. Articular, para poner en marcha, las ***aplicaciones de tecnología de la información***, de controles internos de ciberseguridad. Estos programas también han sido ampliados en otros capítulos del presente trabajo, pero aquí lo orientamos a los riesgos estratégicos. Así, por ejemplo, hacer uso del programa de "Proyectos y Estrategia", o el programa denominado "Estrategia, Proyectos y Resultados" (por ejemplo, software de ***Playtech***, que pueden encontrarse en Monday.com), los cuales dan seguimiento del aseguramiento y de los resultados de las pruebas asociadas con los riesgos estratégicos, en la integración de datos para ayudar a monitorear riesgos y generar reportes. No podemos soslayar la importancia que tienen los programas antivirus (Bitdefender, Norton, McAfee, Kaspersky, Panda, etc.), en cualquiera de sus modalidades, más las adaptaciones para hacerlos a la medida de la empresa, para lo cual hay que preguntarse por sus capacidades de detección de peligros, su rendimiento, sus aplicaciones específicas y amigabilidad, la relación calidad-precio, la protección en tiempo real, la eliminación de programas malignos, de los spyware, de software publicitarios, de secuestro de datos, de ciberestafas, de antifraudes, modos de rescate, protecciones de cámara web, cortafuegos, protección de redes sociales, administración de contraseñas, antirrobo, ayudas técnicas y compatibilidades.

d. En lo personal, me gusta darle relevancia a la ***independencia y criterio desinteresado de expertos.*** Es por ello, que soy fiel creyente de que entes externos (auditores independientes y expertos en ciberseguridad) y otros grupos fuera de la organización, pueden y deben ser considerados como adicionales líneas de defensa, proporcionando aseguramiento a las partes interesadas de la organización, incluyendo los organismos de gobierno corporativo y la alta dirección.

La Ciberseguridad: Consejos para enfrentar riesgos

Hemos deseado incorporar también como parte del texto principal de este trabajo, la redacción de algunas anotaciones diversas de lecturas realizadas sobre el tema conseguidos en internet (y que se listan en la infografía), así como extraídos de la biblioteca E-Libro de la UNESCPA, relacionadas con algunas formas de enfrentar los peligros cibernéticos.

El control interno, dentro de la ciberseguridad, intenta proteger el procesamiento, transmisión y almacenamiento de información de índole digital o informático. No interesa cuánto esfuerzo, empeño o sacrificio hayamos puesto en construir una barrera digital alrededor de nuestro sistema computacional, aún podemos encontrarnos intempestivamente y hallar que esa información artificial, o una copia de esa documentación se haya perdido, que ha sido robada o dañada, malograda o inutilizada, por cualquier serie de accidentes desafortunados o actos malintencionados o maliciosos.

En nuestras organizaciones, tenemos máquinas potentes, pero igualmente poseemos equipos vulnerables. Algunos consejos, en resumen, de control interno, con visión de protección de la informática empresarial, podrían listarse así:

a. **Mantener siempre el sistema operativo actualizado, porque éstos sufren diversos cambios.** Estos mismos sistemas suelen ofrecer sus propias herramientas que permiten que el equipo se actualice de forma automática. Las actualizaciones posibilitan que se corrijan vulnerabilidades, frente a peligros o amenazas, causadas por virus y evitan que se propaguen "softwares" malignos. Un ejemplo claro, del día a día, es el ***"Windows Update"***.

b. **Usar un antivirus y aplicaciones *"Anti-Malware"*, con miras a proteger los equipos informáticos.** En el mercado informático de programas de este tipo, hay una gama diversa. Claro está, estas ayudas pueden ser pesadas en cuanto al espacio que toma en nuestros ordenadores, sean éstos de uso personal, o integrados en una red, o en circuito, comprimidos dentro de un ***"servidor"*** para toda una empresa o parte de ella. Por ello, hay que leer con detenimiento cuáles son las especificaciones mínimas que pueda requerir el antivirus que podríamos adquirir, para que sea instalado y funcione en la velocidad y con la eficacia y efectividad necesarias.

c. **Utilizar programas especializados que realicen la localización del *"malware"***, que nos permita eliminar softwares y aplicaciones (apps) malintencionados. Entre estos programas de ciberseguridad podemos encontrar en el mercado el ***"malwarebytes"***;

d. **Contraseñas seguras.** Hay organizaciones que utilizan contraseñas o códigos de entrada por muchos años, sea para todas las aplicaciones, o algunas de ellas. Esto es un riesgo en el control interno. Desde que se descubre una contraseña, el ***hackeador*** o ciberdelincuente suele descubrir todas las demás. Es bastante común llegar a las oficinas, sean éstas, privadas o públicas, donde se observan papelitos pegados en los monitores o escritorios con los códigos de entrada para insertarse en los sistemas o programas. Esto ocurre hasta en las instituciones financieras. Es un riesgo altísimo para potenciales estafas y fraudes, ya que el usuario, desprevenidamente o sin pericia o sin malicia, deja al descubierto el alma cibernética de la empresa.

e. **Gestión de contraseñas.** Es común el uso de "keepass", cual es un sistema de seguridad de control interno cibernético, que permite proteger las distintas contraseñas de forma segura y generalmente soporta diferentes sistemas operativos o multiplataformas. La idea también es que, en sitios públicos, o pegados a "wifi" de forma remota, tratemos de no entrar de forma directa sino antes hacer "clic" sobre la opción "olvidar contraseña", porque el ***hackeador*** está buscando contraseñas de fácil acceso, que incluyen fechas de nacimiento y nombres de cónyuges e hijos. El gestor de contraseñas te permite ubicar los mejores códigos de difícil hurto;

f. **Activar un *"firewall"*.** Todo sistema operativo debe poseer este dispositivo, que permite al usuario seleccionar el tráfico que entra en tu central o servidor computacional, previniendo ataques de la red. Es recomendable que se active en configuraciones cibernéticas cerradas, para evitar accesos no deseados.

g. **Softwares para evitar secuestro de datos.** Existen programas computacionales para contrarrestar los ***"ramsonware"***. Éstos consisten, como expresamos arriba en el presente trabajo, en programas dañinos que logran provocar restricciones en acceso a determinadas partes o archivos del sistema operativo infectado. De hecho, constituye una de las amenazas más apremiantes hoy en día. Estas intromisiones malignas secuestran archivos confidenciales y se hacen del control de éstas hasta que la víctima pague una extorsión o chantaje para restablecer el funcionamiento del sistema.

h. **Softwares de navegación de privacidad.** Estos sistemas permiten abrir ventanas independientes para entrar de una forma denominada "modo incógnito", de tal manera que un tercero no pueda explorar, y que elimina los datos de las sesiones de navegación por internet, lo cual puede ser preconfigurado. Un buen sistema en ese sentido puede ser, por ejemplo, el ***"Firefox"***.

i. **Copias de seguridad o "back-up".** Dentro del control interno, como parte de la exigencia de ciberseguridad, es imprescindible realizar consistente y constantemente el respaldo de alojamiento de la data de los dispositivos informáticos. Ideal es que el llamado ***"back-up"*** sea automático. En nuestra lectura de material accesible bibliográfico e infográfico, podemos encontrar softwares que se mercadean para cumplir con este control interno de ciberseguridad, tales como ***Cobián Backup***, ***IDrive Cloud Backup***, ***EaseUS***, ***Todo Backup***, **Backup Free**, ***Google Drive Backup*** y ***Cómodo Backup***.

j. **Utilización de softwares para Redes Privadas Virtuales (VPN, en sus siglas en inglés)**, que proveen conexiones seguras y cifradas, para evitar entradas de terceros hackeadores. Según hemos investigado, no es seguro usar VPNs gratuitas. Existen algunos softwares que vienen en conjunto con sus sistemas "madre", como ***"Hide.me"***, ***"TunnelBear"***, ***"Speedify"***, ***"Opera"***, ***"FirefoxVPN"***, ***"ProtonVPN Free", "Windscribe"*** y ***"Hotspot Shield Free VPN"***.

k. **Herramientas de cifrado para USB** (dispositivo de almacenamiento -***U***niversal ***S***erial ***B***us-, que utiliza memoria flash para guardar información y que

se conecta mediante un puerto autónomo de inserción mecánica en los sistemas computacionales, que es modificable muchas veces en su vida útil y que suele herirse de virus con facilidad). Es recomendable que los discos duros y memorias USB estén encriptados con algún software específico de 'caracteres cifrados' para que terceros no puedan acceder a su contenido fácilmente. Ejemplos: "Boxcryptor", "Veracrypt", "Axcrypt", "Filevault 2" y "Bitlocker".

l. **No utilizar softwares piratas.** Dentro de la multiplicidad de infografía seleccionada, varias de ellas enfatizan en que debemos siempre usar softwares originales, puesto que los softwares llamados "piratas" acaban siendo fuentes de vulnerabilidad y maximizan probabilidades de tener futuros problemas.

m. **Utilización de varios servidores para evitar sustracción íntegra.** Un agregado de carácter personal, de mi autoría, es que debemos emplear diferentes sistemas informáticos para diversas funciones. Esto evita que, en caso de hackeo indeseado, toda la información empresarial llegue a las manos de los ciberdelincuentes. Manejar a la organización con informática separada, es decir, una para mensajes de correo electrónico, otra para contabilidad, otra para recursos humanos, otra para los programas de trabajo de campo, otra para archivos, y demás, aunque no evita que tengamos daños de índole dinerario, reputacional, periodístico, congelamiento del sistema, o cualesquiera consecuencias, éstas causarían detrimento a una fracción de la organización, evitando una catástrofe generalizada.

n. **Talleres educativos al recurso humano.** Nada de lo anteriormente expuesto, como instrumentos para hacerle frente a los riesgos cibernéticos, sería de real utilidad, si no buscamos el compromiso del personal de la organización, en búsqueda de la seguridad cibernética, en mutua conciencia de la relevancia del cuidado necesario. Los códigos de uso o comportamiento en los ordenadores individuales y colectivos deben ser una práctica estándar ineludible. Nos referimos a la prohibición de abrir adjuntos que no vengan pre-

cifrados, o que no sean anticipadamente conocidos. Esto suele encontrarse a través de cursos cortos, pero muy dirigidos, que busquen ese matrimonio que se necesita con todo el personal que maneja ordenadores informáticos, buscando una responsabilidad individual de cada uno de ellos.

Los seis componentes para la evaluación de riesgos de ciberseguridad

Como parte de nuestra investigación, pasamos a detallar los seis componentes de evaluación de los riesgos de ciberseguridad, así:

a. **Procesos de Gobierno.** La alta gerencia debe esclarecer roles y tareas, trabajar en colaboración, establecer qué es asumido y tolerado, planificar la continuidad del negocio, responder velozmente y establecer conciencia y cultura frente a las latentes amenazas. La Dirección debe recibir de parte de la sección encargada de la Administración del Riesgo, los análisis de los riesgos cibernéticos, conforme se examinen las probabilidades y los posibles impactos o severidades, después de contemplarse las amenazas, las vulnerabilidades internas y el entorno estratégico de la organización (en sus diversos factores internos y externos), con el supuesto de que estamos atravesando por una identificación de estos riesgos cibernéticos y la estricta evaluación de los mismos. En virtud de esto, se establecen procesos para el establecimiento de controles internos y la valoración de estos controles, para poder descifrar con los expertos informáticos, los mejores tratamientos. Y de todo ello, inventariar los riesgos inherentes cibernéticos, enfrentarlos contra la demostración de la eficacia de sus controles (para concebir cuáles son los riesgos residuales), para entonces poder engendrar tablas de niveles de riesgo, así como mapas de calor de riesgos inherentes y mapas de calor de riesgos residuales cibernéticos.

   El análisis económico, el apetito del riesgo y la asignación de funciones debe realizarse por la alta gerencia, en vías de determinar cuáles deben ser las políticas empresariales frente al flagelo del riesgo cibernético. Las metodologías **ISO** contribuyen mucho con COSO-ERM para confrontar estas realidades de ciberdelincuencia, y resumirlas para los que toman decisiones estratégicas en lo más alto **-gerencialmente hablando-** de las organizaciones.

b. **Inventario de activos.** Tener en cuenta los elementos tales como tipos de transacciones y configuraciones de tecnología; clasificaciones de riesgos; entornos; repositorios de infraestructura de activos de tecnología; aplicaciones; y relaciones externas.

c. **Configuraciones estándares de seguridad.** Softwares de configuración centralizados y automatizados, softwares de gestión, evaluaciones siempre basadas en el riesgo, más procesos de aplicación de parches.

d. **Gestión de acceso a la información.** Movimientos de empleados, delegación de autoridad, segregación de funciones, acceso a usuarios, inventario de sucesos de suplantación de identidad, acceso a privilegios; y accesos a datos clave.

e. **Respuesta y medidas de remediación.** Comunicación y seguimiento de las resoluciones en respuesta a sucesos.

f. **Supervisión continua.** Evaluaciones de la detección de vulnerabilidades en cuanto a personas de acceso, vulnerabilidades en cuanto a los sistemas de alto riesgo (malware e infiltración de datos), sistemas de uso externo, riesgos de terceros, poner en práctica pruebas de penetrabilidad, simulacro para medir respuestas a incidentes, más riesgos emergentes.

El activo valioso de la Propiedad Intelectual frente al riesgo cibernético

Como necesidad académica en el desarrollo de la presente investigación, nos adentramos en el tema de la Propiedad Intelectual. Sobre todo, exploramos el asunto de las pérdidas financieras provocadas por ataques cibernéticos.

No hay que ir muy lejos en el mundo. En Panamá, un asalto cibernético (hackeo), acontecido durante el año 2015, pero dado a la luz pública un 3 de abril de 2016, hecho a los sistemas computacionales de la firma forense Mossack & Fonseca, empresa panameña que valía aproximadamente US$900 Millones y que facturaba cerca de US$200 Millones anuales, deterioró en tiempo récord su reputación. En

cuestión de pocas semanas, Mossack & Fonseca perdió su capacidad de contar con bancos que le proveyesen servicios y su clientela fue absorbida enteramente por la competencia. La empresa fue pulverizada. Por la connotación mediática que significó el hackeo, las autoridades jurisdiccionales de investigaciones criminales se vieron obligadas a comenzar procesos en materia penal. Hoy en día, y después de revisados más de 340,000 expedientes, los cuales consistían, teóricamente, en relaciones delictuosas, que significaban 11 Tetra- Gigabytes de documentación, solamente pudieron emprender un (1) proceso en contra de la empresa hackeada, la cual seguramente será declarada inocente por la autoridad judicial de todo comportamiento delictivo. En conclusión, la empresa, aunque de comportamiento cívico, ético y correcto, no contaba con sistemas de control interno de ciberseguridad, ni políticas adecuadas a nivel estratégico. Su apetito de riesgo cibernético era en exceso alto.

Varios son los asuntos que debemos subrayar en este tema de valoración de la importancia de la propiedad intangible:

Seguridad de que podemos prevenir amenaza cibernética. Con ello, realizar inventarios de los programas que poseemos, hacer pruebas, y mantener informados a todos los actores de la organización de forma vertical y horizontal.

Recalcar la relevancia ante la Junta Directiva y Gerencia General. En este tema, debemos preguntar constantemente cuál es la evaluación de la auditoría interna respecto a la capacidad para asegurar su propiedad intelectual; si hay procedimientos formales a seguir en caso de violaciones; si hemos evaluado los riesgos intelectuales; si tenemos destinados recursos y financiamiento para contrarrestar los riesgos cibernéticos; si tenemos inventariadas las propiedades intelectuales; si la junta y/o gerencia tiene suficiente tiempo para comprender los riesgos; y cuál es el valor en juego, razonando si éstos podrían aniquilar a la empresa.

Entendimiento de la relevancia en todos los niveles. Es decir, explicar en el idioma de todos en la organización, de lo grave que podría ser un hackeo de propiedad intelectual.

Esfuerzo holístico. Es decir, dejar aparte la idea rezagada de que el Departamento de Tecnología de la Información (TI), es la responsable de los

riesgos cibernéticos, y tener presente que el riesgo tecnológico y cibernético es, en general, igual que el físico. La única diferencia es que es 'electrónico' en lugar de 'material'. Es 'incorpóreo' en vez de 'somático'.

Valorar que se trata de una amenaza invisible. Conocer que los tipos más comunes de individuos detrás de las amenazas son: hackers privados, hackers apoyados por el Estado, atacantes criminales y hackers con ideales (ambientalistas o defensores de derechos humanos). Y que los medios más frecuentes de irrupción son los programas maliciosos como "Troyano", gusanos, virus, softwares espías, phishing (obtención de contraseñas), y ataques de bloqueo de sitios web, que entran vía correo electrónico, teléfonos celulares, o accesos a ventanas informáticas.

Estar conscientes de las pérdidas. Éstas pueden ser: Financieras, robo de propiedad intelectual, daño reputacional, fraude y exposición legal.

Funciones del Auditor Interno en su rol de control en la ciberseguridad

Como parte del estudio de la ciberseguridad, con énfasis en el Control Interno dentro de dicha ciberseguridad, además de enfocarnos en COSO (Sistema de Control Interno 2013 Gestión de Riesgos Empresariales – ERM, 2017 y anteriores) nos adentramos en Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés: National Institute of Standards and Technology), del Departamento de Comercio de los Estados Unidos. A través de diversas búsquedas de material bibliográfico, listado en la sección del final del trabajo, entre ellos un interesante trabajo de los profesores Charlie Wright y Lynn Fountain del Instituto de Auditores Internos (IIA, por sus siglas en inglés), podemos resumir que los auditores internos deben reunir diversos desempeños ocupacionales en su rol de enfrentar el riesgo cibernético:

a. **Estar atento de los enfoques de ciberseguridad de la NIST y de otros modelos de control interno.** A medida que la tecnología avanza, las tareas de los auditores internos evolucionan. Por ello, el auditor debe estar continua y constantemente informado de las diversas formas de enfrentar estos flagelos y, por ello, estar familiarizado con los múltiples lineamientos para un mejor control interno organizacional, como COSO (Estados Unidos, cual es el "Comité de Organizaciones Patrocinadoras de la Comisión TREADWAY"),

COCO (Canadá), Cadbury (Reino Unido), Vienot (Francia), Peters (Holanda), KING (Sudáfrica), MICIL (adaptación del COSO para Latinoamérica), u otros, tales como ISACA-RISK-IT (The Information Systems Audit and Control Association) y la organización (ISO 31000 y demás).

b. **El uso de la experiencia para aprender lecciones.** Es imperioso evaluar las lecciones aprendidas en incidentes que causen perjuicio. Las fases de recuperación producen respuestas a las vulnerabilidades.

c. **Responder a incidentes.** La búsqueda de solución debe ser muy rápida. El impacto podría ser desastroso. Los auditores internos deben conocer los desafíos y guiar con perspectivas independientes.

d. **Supervisar los procedimientos de detección.** Aunque la realización de los procedimientos de detección de riesgos cibernéticos es responsabilidad de la dirección, los auditores internos pueden y deben probar dichos procedimientos para corroborar que están bien diseñados y pueden operar acordemente.

e. **Reconocer y resguardar los activos en riesgo cibernético.** El auditor interno debe buscar que su organización priorice e implante salvaguardas, dando seguimiento a su evaluación de forma vertical, determinando si está siendo eficaz, integrando los riesgos cibernéticos al plan de auditoría, justipreciando si el Consejo de Auditoría y/o la Dirección (Gerencia General) ha desarrollado una estrategia integral contra el ciber-riesgo, calculando capacidades para gestionar activos tangibles e intangibles afectados en caso de ataque cibernético, realizando auditorías individuales por departamento o sección; y dar énfasis de que los enfoques deben ser siempre estructurados.

f. **Conocer detalladamente el enfoque que utiliza la respectiva organización** (cualquiera de los modelos, sea COSO, NIST, ISO, ISACA o algún otro), de tal forma que haya un protocolo estándar en caso de embestida cibercriminal.

g. **Capacitarse en amenazas y fraudes cibernéticos.** El conocimiento es poder.

Director Ejecutivo de Auditoría (DEA). Relevancia y funciones

El Instituto de Auditores Internos (IIA), en sus múltiples publicaciones, pone énfasis en la importancia de contar con un Director Ejecutivo de Auditoría (DEA), que priorice en una comunicación eficiente entre las líneas de defensa frente a las ciber-amenazas y que los miembros del Consejo de Auditoría estén informados

continuamente sobre los desafíos en materia de ciberseguridad, cibercrimen, ciber-riesgos y ciberdelincuencia. Asimismo, generar conciencia sobre la necesidad de poseer estructura de gobierno corporativo adecuada para enfrentar los riesgos, asegurarse de que hay elementos suficientes para la gestión de riesgos y analizar si hay grados suficientes de aceptación de los riesgos para la correcta toma de decisiones estratégicas. De igual importancia es el análisis de datos para la detección del fraude.

El Ciber riesgo en Panamá

Tenemos que destacar que nuestro País no está libre de los ataques cibernéticos de todo tipo, teniendo un centro bancario de gran importancia, estas instituciones se convierten en blancos deseados por los ciberdelincuentes, por ello en nuestro país son cada vez más comunes ataques a personas por medio de pirshing o ransomware, según (La Estrella de Panamá, 'phishing' Y 'ransomware', Los ciberataques más comunes a la Banca Panameña 2023) “Durante los últimos seis meses, la banca panameña reportó 1.313 ataques por semana de ciberataques, mientras que el sector de gobierno presentó 803.” Estas estadísticas son preocupantes especialmente porque sabemos que cada día estamos más inmersos en aplicaciones en los dispositivos ya sea por trabajo o esparcimiento.

Para el comercio en general de nuestro País es de gran importancia prevenir todo tipo de delitos cibernéticos para esto se han adelantado propuestas para definir y poner en práctica normas legales para la regulación del comercio cibernético y los criptoactivos. Para esto se ha presentado el proyecto de ley 697 sobre las criptomonedas, sin embargo, no ha encontrado suelo fértil para avanzar, según (La Estrella de Panamá, *Expertos Hablan sobre la necesidad de una regulación de criptoactivos en panamá* 2023) “Actualmente este proyecto de ley se encuentra a la espera de un fallo por parte de la Corte Suprema de Justicia, después que el Órgano Ejecutivo lo objetara por inexequible. y precisó que la iniciativa legislativa requiere “adecuación” a las normas que regulan el sistema financiero y el modelo monetario panameño.” Esta falta de regulación coloca a nuestro país en una desventaja a no poder regular la actividad económica, sino que además estamos imposibilitados para reclamaciones por medio de tribunales hacia los responsables de dichos delitos.

Conclusiones:

Como preparadores de trabajos de investigación, confiamos más en la pluralización del término conclusión. Por lo general, no se utiliza en singular, sino en plural: Conclusiones.

Desenvolvemos nuestras conclusiones listando lo que consideramos de mayor relevancia en esta investigación, y que debe servirnos de principales patrones o ideas principales e ilustrativas a seguir en el tema el papel del control interno dentro de la ciberseguridad basado en el Modelo COSO - ERM:

1. El control interno dentro de COSO ERM - 2017 hizo importantes añadiduras respecto a la necesidad de enfrentar riesgos en materia de ciberseguridad, lo cual puede evidenciarse en sus componentes, sus principios, su marco conceptual y sus objetivos de actualización;
2. Las principales implicaciones en los avances de COSO ERM - 2017 respecto a la ciberseguridad se basan en la concienciación en la cultura organizacional y su relevancia para la toma de decisiones estratégicas;
3. Los fraudes cibernéticos van de la mano con los temas de ciber-riesgos y su necesario control interno para enfrentarlos. Para neutralizarlos o contrarrestarlos, debemos implantar controles físicos, técnicos y administrativos;
4. Las transformaciones de COSO ERM 2017 consisten primordialmente en orientar el control interno hacia la ciberseguridad, utilizar más consistentemente normas ISO y mayores y mejores tecnologías de la información, así como agenciar a expertos para obtener sus criterios independientes y desinteresados;
5. Los auditores internos no pueden soslayar en sus funciones, los consejos, que son articulados por los eruditos en la materia, sobre los mecanismos o instrumentos para enfrentar los riesgos cibernéticos, entre ellos, actualizarse, usar consistentemente contraseñas cambiantes, herramientas de seguridad, encriptaciones, códigos cifrados, copias de seguridad, softwares de privacidad, entre tantas otras armas;
6. Los encargados del control interno, que somos todos, pero priorizando en el Auditor Interno, el Comité de Auditoría y el Director Ejecutivo de Auditoría, debemos dar primacía o preponderancia a los principales componentes para

la evaluación de riesgos de ciberseguridad y, entre éstos, las configuraciones estándares y la supervisión continua;

7. No debemos nunca quitarle trascendencia al peso que tiene la propiedad intelectual o intangible en las organizaciones;
8. El rol del control interno en la ciberseguridad suele recaer en la figura del Director Ejecutivo de Auditoría, cuyas funciones son trascendentales. La ejecución de estas funciones no debe considerarse como una meta aislada, sino como parte de los objetivos existenciales o estratégicos del negocio.

Concluimos, que debemos decir adiós al esquema de pensamiento anterior, que la ciberseguridad era una responsabilidad aislada de los gerentes de informática y pasar a un nuevo enfoque entendiendo que es responsabilidad de todos.

Bibliografía / Infografía

3Ciencias (n.d.). Introducción a la Seguridad Informática [Web page]. Retrieved from http://www.3ciencias.com

AEC (n.d.). Control Interno – COSO [Web page]. Retrieved from http://www.aec.es

ASC (n.d.). Concepto de cibernética [Web page]. Retrieved from http://www.asc-cybernetics.org/foundations/timeline.htm

B2B México. (2017). COSO, Riesgos de Negocio y Seguridad Cibernética, ¿Cómo se relacionan? Recuperado de https://www.b2bmexico.net/post/2017/10/19/riesgos-de-la-seguridad-cibernética-y-los-objetivos-del-negocio-como-están-relacionados

Canals, D. (2021). Ciberseguridad: Un nuevo Reto para el Estado y los Gobiernos Locales. Editorial Wolters Kluwer.

CEUPE (n.d.). ¿Qué es el cibercrimen? [Web page]. Retrieved from http://www.ceupe.com

Consuegra de Sucre, D. (2022, October 31). Consejos de Seguridad Informática. Diario La Prensa.

Dell (n.d.). Soluciones de Ciberseguridad [Web page]. Retrieved from http://www.dell.com

Departamento de Comercio de EE. UU. Marco de Ciberseguridad NIST. Recuperado de www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

Estupiñán, R. Administración de Riesgos y E.R.M. y la auditoría interna. Eco ediciones. Recuperado de https://www.ecoeediciones.mx/wp-content/uploads/2015/07/Administracion-de-riesgos-ERM-y-la-auditor%C3%ADa-interna-2da-Edici%C3%B3n.pdf

Gayoso Martínez, J. (2020). Ciberseguridad. Editorial del CSIC - Consejo Superior de Investigaciones Científicas.

Global Suites Solutions. Automatización del Modelo de las 3 Líneas de Defensa. Recuperado de https://www.globalsuitesolutions.com/es/automatizacion-modelo-3-lineas-defensa/

Gómez, N. (2021). Normativa de Ciberseguridad. RA-MA Editorial.

Grech, N. Estrategias de Marketing digital en un Entorno Ciberseguro. RA-MA Editorial.

Ibercaja (n.d.). ¿Qué es ciber-riesgo? [Web page]. Retrieved from http://www.ibercaja.es

IBM (n.d.). ¿Qué es ciberseguridad? [Web page]. Retrieved from http://www.ibm.com

INESE (n.d.). ¿Qué son los ciber-riesgos y cuáles son sus características? [Web page]. Retrieved from http://www.inese.es

Institute of Internal Auditors (IIA). Las Tres Líneas de Defensa para una Efectiva Gestión de Riesgos y Control. Recuperado de https://www.funcionpublica.gov.co/eva/admon/files/empresas/ZW1wcmVzYV83Ng==/imagenes/93/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control%20Spanish.pdf

ISOTools. ¿Cómo ha cambiado el nuevo COSO ERM 201

Jaramillo, O.A. (2023) *Cada día 13 personas son Víctimas de Estafa; El Ciberdelito desafía a la justicia*, *La Prensa Panamá*. La Prensa Panamá. Available at: https://www.prensa.com/sociedad/cada-dia-13-personas-son-victimas-de-estafa-el-ciberdelito-desafia-a-la-justicia/ (Accessed: April 11, 2023).

Kaspersky (n.d.). Qué es el cibercrimen, cómo protegerse del cibercrimen [Web page]. Retrieved from http://www.latam.kaspersky.com

La Estrella de Panamá, G. E. S. E. (2023, March 24). *'phishing' Y 'ransomware', Los ciberataques más comunes a la Banca Panameña*. La Estrella de Panamá. Retrieved April 11, 2023, from https://www.laestrella.com.pa/economia/230324/phishing-ransomware-ciberataques-comunes

La Estrella de Panamá, G.E.S.E. (2023) *El 'phishing' como delito financiero (ii)*, *La Estrella de Panamá*. Available at: https://www.laestrella.com.pa/opinion/columnistas/230409/phishing-delito-financiero-ii (Accessed: April 11, 2023).

La Estrella de Panamá, G.E.S.E. (2023) *Expertos Hablan sobre la necesidad de una regulación de criptoactivos en panamá*, *La Estrella de Panamá*. Available at: https://www.laestrella.com.pa/economia/230320/expertos-hablan-necesidad-regulacion (Accessed: April 8, 2023).

La Salle (n.d.). Concepto de Cibernética [Web page]. Retrieved from http://www.ingenieria.lasalle.mx

Miranda-Partners. ¿Qué son las tres líneas de defensa en una organización? ¿Cuál es el rol de Compliance en estas líneas? Recuperado de https://miranda-partners.com/es/que-son-las-tres-lineas-de-defensa-en-una-organizacion-cual-es-el-rol-de-compliance-en-estas-lineas/

Moreno, M. (2022). Gestión de Incidentes de Seguridad. RA-MA Editorial.

OVNI (n.d.). Ciberseguridad – Expertos en Ciberseguridad [Web page]. Retrieved from http://www.ovni.com

PwC México. Actualización COSO ERM 2017. Implicaciones de COSO para el sector de energía. Recuperado de www.pwc.com/mx

PwC México. Cambios e implicaciones de COSO en ciberseguridad. Recuperado de www.pwv.com/mx

PwC México. Implicaciones de COSO en ciberseguridad y privacidad. Recuperado de www.pcw.com/mx

S2 Grupo (n.d.). La Propiedad Intelectual y su relación con la ciberseguridad [Web page]. Retrieved from http://www.s2grupo.es

Scribd (n.d.). Propiedad Intelectual y Ciberseguridad [Web page]. Retrieved from http://www.scribd.com

Servicio (n.d.). Modelos Contemporáneos de Control Interno. Fundamentos [Web page]. Retrieved from http://www.servicio.bc.uc.edu.ve

SoftwareLab (n.d.). Definición y los 5 principales cibercrímenes [Web page]. Retrieved from http://www.softwarelab.org

Téllez, R. (2015). Investigación y Prueba del Ciberdelito [Doctoral dissertation, Universidad Politécnica de Cataluña]. Retrieved from http://www.tdx.cat

Tigo (n.d.). Ciberseguridad Informática – Seguridad Cibernética [Web page]. Retrieved from http://www.tigo.com

Turner, L. (2002, June). Control Self-Assessment: A Practical Guide. Internal Auditor, 59(3), https://link.gale.com/apps/doc/A87430386/AONE?u=anon~e6b0221f&sid=bookmark-AONE&xid=6d10c836.

UNODC (2013). Compendio de Ciberdelincuencia Organizada-UNODC. Retrieved from http://www.unodc.org