NOVUM, revista de Ciencias Sociales Apliacadas
ISSN: 0121-5698
ISSN: 2357-4933
rev_novum_fadman@unal.edu.co
Universidad Nacional de Colombia
Colombia

Caamaño Fernández, Enier Enrique; Gil Herrera, Richard de Jesús
Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional
NOVUM, revista de Ciencias Sociales Apliacadas, vol. I, núm. 10, 2020, -Junio, pp. 61-80
Universidad Nacional de Colombia
Colombia

Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional

Cybersecurity risk prevention from forensic auditing: combining organizational human talent

Fecha de recibido: 14/06/2019 *Fecha de aceptación: 3/11/2019*

Enier Enrique Caamaño Fernández. Estudiante del Doctorado en Proyectos en la Universidad Americana de Europa – UNADE, Magíster en Gerencia de Empresas. Profesional G08 del Servicio Nacional de Aprendizaje - SENA, Valledupar, Cesar – Colombia. **Correo electrónico:** enierc8@hotmail.com **ORCID:** https://orcid.org/0000-0003-0280-1453
Richard de Jesús Gil Herrera. Doctorado en Ciencias de la Computación y Tecnologías de Información (UGR-España). Docente de la Universidad Americana de Europa – UNADE. Andalucía– España. **Correo electrónico:** richard.dejesus@aulagrupo.es **ORCID:** https://orcid.org/0000-0002-8207-8519

Cómo citar este artículo
Caamaño Fernández, E.E., y Gil Herrera, R.J. (2020). Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional, *NOVUM*, 1(10), 61 - 80.

Resumen

Objetivo: Con el presente artículo de investigación se busca analizar cómo las Tecnologías de la Información y de las Comunicaciones (TIC) han jugado un papel esencial en la gestión del conocimiento del capital intelectual que, a partir de las competencias adquiridas, permiten a las organizaciones modernas, mediante la auditoria forense blindarse oportunamente para reaccionar ante cualquier ciberataque que afecte la operación y competitividad dentro de este mundo globalizado. **Metodología:** Esta investigación fue de tipo exploratoria, descriptiva y documental sobre los temas investigados, los cuales, en forma general, tienen grandes implicaciones en la ciberseguridad organizacional, mediante mecanismos de prevención de la gestión del conocimiento y la auditoría forense. **Hallazgo:** Los resultados mostraron de manera esquemática y/o gráfica que la ciberseguridad organizacional integrada a la auditoría forense y, además, a la gestión del conocimiento como medida para la prevención y detección del fraude, la corrupción y delitos informáticos, garantizan las pruebas para los procesos judiciales y los activos de información para la toma oportuna de decisiones por parte de los niveles estratégicos, tácticos y operativos de las organizaciones modernas. **Conclusión:** La ciberseguridad organizacional como instrumento para la prevención, detección de operaciones fraudulentas y sospechosas, fungiría de

garante de las operaciones y en la toma de decisiones del capital intelectual al conjugarse bajo un enfoque sistémico, con la auditoría y la gestión del conocimiento. **Palabras clave:** Auditoría de gestión; Ciencias de la información; Corrupción; Tecnologías de la información.

Abstract

Objective: With the present article of research it seeks analyze how Information and Communication Technologies (TIC) have played an essential role in the management of intellectual capital knowledge that, based on the competences acquired, allow modern organizations through forensic auditing to shield themselves in a timely manner to react to any cyber-attack, that affects the operation and competitiveness within this globalized world. **Methodology:** This research was exploratory, descriptive and documentary on the topics investigated, which, in general, have great implications in organizational cybersecurity, through mechanisms for the prevention of knowledge management and forensic auditing. **Finding:** The results showed schematically and / or graphically that organizational cybersecurity integrated with forensic auditing and, in addition, knowledge management as a measure for the prevention and detection of fraud, corruption and cybercrime, guarantee evidence for processes judicial and information assets for timely decision making by the strategic, tactical and operational levels of modern organizations. **Conclusion:** Organizational cybersecurity as an instrument for the prevention, detection of fraudulent and suspicious operations, would act as guarantor of operations and in the decision making of intellectual capital when combined under a systemic approach, with audit and knowledge management. **Keywords**: Management audit; Information sciences; Corruption; Scientific Information.

Introducción

La globalización de la economía ha incidido sustancialmente en las condiciones de vida de la sociedad, en el desarrollo económico de las naciones, como en la cultura empresarial de las organizaciones modernas que, a través de los avances tecnológicos, se han visto expuestas a riesgos y amenazas, que día tras días son vulnerables frente al cumplimiento efectivo de sus operaciones. Se vuelve perentorio para tales organizaciones, la salvaguarda de los recursos, el logro de los objetivos y metas trazadas en el corto, mediano y largo plazo, para satisfacer las necesidades y expectativas de los clientes, grupos de interés y partes interesadas, conllevando con ello, la no potencialización de la cadena de valor en la producción de bienes y servicios para ser competitivas y distintivas en el mercado.

En consecuencia, si bien los avances de las Tecnologías de la Información y las Comunicaciones – TIC, han traído resultados positivos a nivel mundial en la revolución de los negocios y en el mejoramiento de la calidad de vida de la población en sus diferentes contextos, no obstante, conllevan también aspectos negativos. Es de interés específico, las

amenazas de ciberataques que, en algunos casos, por no tener medidas de prevención y control, las empresas se han visto abocadas mediante el uso indebido del poder, a realizar maniobras fraudulentas, sobornos, corrupción y delitos informáticos, para incursionar en nuevos mercados, con capacidades técnicas y recursos para apoderarse de este y así, obtener un beneficio de tipo político y/o económico en el contexto estatal.

De ahí el surgimiento de la auditoría forense como recurso de prevención de los riesgos de ciberseguridad que, conjugando talento humano con altos niveles de competencias, permite blindar a las organizaciones modernas frente ataques informáticos y actos indebidos, que puedan traer consecuencias graves en la continuidad del negocio y esta a su vez se vea afectada en su posición distintiva frente a los competidores, en un entorno económico y tecnológico que evoluciona a gran velocidad.

En ese sentido, cualquier empresa, de acuerdo con las exigencias y complejidad de los negocios que demanda la economía moderna, están expuestas cada vez más a amenazas y a ser vulnerables frente a los ciberataques; si no cuentan con un robusto sistema de prevención y control de riesgos de ciberseguridad podrían poner en peligros las finanzas para atender los planes estratégicos y financieros de largo plazo por parte de los niveles estratégicos, gerenciales y operativos de la organización.

1. ¿Por qué hablar de ciberseguridad?

Los avances de la tecnología de la información y las comunicaciones – TIC, han traído grandes transformaciones para la globalización de la economía, las organizaciones y la sociedad en general, obligándolas no solo en asumir los nuevos desafíos que demandan las mismas desde el plano social, político, económico y cultural; además, la adopción de medidas que garanticen la seguridad de la información, los recursos y la infraestructura que son esenciales para la toma oportuna de decisiones en el corto, mediano y largo plazo. Por ello, el uso de las TIC "conlleva serios riesgos y amenazas que pueden afectar a la Seguridad Nacional" (Leiva, 2015, p. 161).

En ese sentido, las organizaciones modernas hoy en día no solo son ajenas a este tipo de problemas, sino que también son vulnerables frente a los activos de información, los cuales son determinantes para la continuidad de las operaciones, la credibilidad y la confianza ante los grupos de interés. Por otro lado, se ven abocadas a afrontar problemas de fraude, soborno, corrupción y delitos informáticos, que notoriamente pueden lesionar las finanzas para satisfacer las necesidades empresariales y sociales que demandan los clientes y partes interesadas. No obstante, "las empresas si no implementan medidas de ciberseguridad y gestionan el riesgo en la infraestructura tecnológica como en los procesos de negocio**,** estarán amenazadas permanente, que de aprovechar sus vulnerabilidades podrían comprometer

seriamente sus activos de información" (Santiago y Allende, 2017, p. 3).

En suma, el objetivo principal de la presente investigación es explorar como la Auditoría Forense aprovecha el Talento Humano para prevenir los riesgos de ciberseguridad organizacional. Se analizan para ello, los distintos antecedentes de investigación, así como los fundamentos teóricos que cimentan los temas seleccionados sobre prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional. Se pretende entonces cumplir con los siguientes objetivos específicos: a) Identificar las características de los riesgos de ciberseguridad organizacional; b) Establecer medidas de control que permitan garantizar la ciberseguridad organizacional; c) Analizar las competencias del talento humano para administrar la ciberseguridad organizacional; d) Formular lineamientos para mejorar la ciberseguridad organizacional, a partir de la gestión del talento humano y la auditoría forense.

Como resultado de los objetivos propuestos, se plantean las siguientes hipótesis para dar respuesta a la investigación realizada: ¿Existen características para identificar los riesgos de Ciberseguridad organizacional? ¿Existen medidas de control que permitan garantizar la ciberseguridad organizacional? ¿Existen competencias del talento humano para administrar la ciberseguridad organizacional? ¿Existen lineamientos para mejorar la ciberseguridad organizacional, a partir de la gestión del talento humano y la auditoría forense?

1.1 Ciberseguridad organizacional

En este mundo globalizado, las organizaciones, los estados y la sociedad en general, han sido amenazadas por ciberataques, lo cual, desde el contexto económico, político y social, representan vulnerabilidades que inciden sustancialmente no solo en la toma de decisiones, sino también, en la estabilidad administrativa y económica para generar confianza ante los grupos de interés. De ahí que, los problemas de ciberseguridad no deben analizarse de manera aislada sino mediante un enfoque sistémico e integral que examine los objetivos estratégicos del negocio, la administración de riesgo, la gobernanza, así como, la psicología organizacional, de tal forma que se determine la situación real del nivel de exposición, con el fin de establecer la línea base para asumir e implementar medidas de prevención y control al respecto.

Por ello, la gobernanza de un sistema de seguridad requiere que se examinen tres factores fundamentales: "seguridad como condición, institucionalidad como medio y desarrollo como objetivo" (Sancho, 2017, p. 8). En este contexto, la ciberseguridad constituye una condición requerida, por cuanto facilita a la ciudadanía en general, empresas públicas y privadas, beneficiarse del uso del ciberespacio a través de las TIC, para compartir información entre los distintos actores sociales. Asimismo, surge también, ante el incremento del uso del

ciberespacio como fuente de interacción social como resultado de la constante innovación de la globalización de la economía y; por último, se comporta como base de datos para el almacenamiento de información que, a través de un análisis técnico efectuada por expertos, es compartida en diferentes formatos disponibles en el ciberespacio.

Los constantes cambios efectuados en innovación en el ciberespacio, ha facilitado el incremento de usuarios en I*nternet*, redes sociales y plataformas tecnológicas, por lo cual, uno de ellos, es el efectivo uso de todo el potencial de *Internet*, tal como indica la Unión Internacional de Telecomunicaciones – UIT (2016) en el reporte anual "Medición de la sociedad de la información":

> Usuarios de *Internet* con niveles educativos más altos utilizan servicios más avanzados, como los de cibercomercio y los servicios financieros y gubernamentales en línea, en mayor grado que los usuarios de *Internet* con niveles de educación e ingresos inferiores, quienes usan *Internet* sobre todo con fines lúdicos y comunicativos (En Sancho, 2017, p. 9).

Bajo ese contexto, al considerarse el ciberespacio un bien público para la sociedad moderna frente a los inminentes factores de riesgos que demanda el mismo, es necesario que las autoridades de cada Estado a nivel mundial, establezcan lineamientos y procesos de entrenamiento para que los ciudadanos de los diferentes estratos sociales, adquieran las competencias requeridas para el uso pleno de las herramientas disponibles en dicho espacio "que garanticen condiciones mínimas de seguridad –según estándares internacionales- para que toda la población pueda usarla en forma confiable" (Sancho, 2017, p. 10). De hecho, "[…] existe una preocupación generalizada acerca de las amenazas que se ciernen sobre estos elementos críticos para el funcionamiento de las sociedades modernas y su capacidad para enfrentarse a ellas (Carrasco y Puerta, 2013, p. 52).

Por consiguiente, "dada la cantidad de datos, la perecibilidad de los datos, la rotación de tecnología y la multitud de partes interesadas e información involucrada, la ciberseguridad es particularmente un problema de Gestión del Conocimiento" (Tisdale, 2015); también, se constituye en un problema de orden local, regional, nacional e internacional. Por esa razón, se convierte en una herramienta eficaz de suma importancia para blindar a las organizaciones frente amenazas y vulnerabilidad ocasionadas por ciberataques existentes en el ciberespacio. De ahí que, "los distintos perfiles de atacantes explotan las vulnerabilidades tecnológicas con el objeto de recabar información de valor para cometer ilícitos, como así también para amenazar los servicios básicos que pueden afectar al normal funcionamiento de un país" (Leiva, 2015, p 161).

Según el reporte Digital en 2018 de Hootsuite 1, en 2017 hubo un total de 8.485 millones de dispositivos conectados a *Internet*, despertando en las empresas y personas la necesidad de utilizar el

ciberespacio[1]. En este contexto, la delincuencia también ha encontrado importantes ventajas, toda vez que desde el anonimato se facilita la realización de ataques cibernéticos desde cualquier lugar del mundo y se reduce la probabilidad que estos sean anticipados y descubiertos. El aumento de los ataques cibernéticos es inminente. Según Kaspersky, en América Latina crecieron en un 59% entre 2016 y 2017 (Asobancaria, 2018). Además, cada vez son más diversos, sofisticados, potentes y con mayor alcance e impacto; en Colombia, de acuerdo con un informe del Centro Cibernético Policial, el cibercrimen en el país aumentó 28,3% en 2017 (Santos, Guisado y Morán, 2017).

Es por esto que las organizaciones modernas para afrontar estos problemas, no solo necesitan analizar las amenazas y vulnerabilidades a que están expuestas, también requieren la arquitectura empresarial y tecnológica, de tal forma que se blinden las finanzas para garantizar que los bienes y servicios producidos satisfagan las necesidades de los grupos de valor. Por ello, para su respectivo control, "requiere, de un talento humano adecuado, con conocimiento profundo de la ciberdelincuencia y de las competencias necesarias para trabajar en pos de su prevención e investigación, ya sea en el ámbito policial o en el empresarial" (Santos, Guisado y Morán, 2017, p. 237).

En efecto, para contrarrestar este flagelo, las organizaciones deben concebir la ciberseguridad como un enfoque integral y holístico necesario para garantizar la seguridad de la plataforma estratégica, tecnológicas y sus finanzas en todos sus aspectos, de tal manera que, se proteja la estabilidad económica y social ante los grupos de interés para su continuidad en el mercado. De donde resulta que "la gestión de la seguridad de los riesgos de la información es un área que se mueve constantemente para responder a nuevas amenazas, estándares y tecnologías" (Jirasek, 2012, p. 1). No obstante, pese a que la tecnología es una pieza fundamental de cualquier estrategia de gestión de riesgos y de seguridad corporativa, la misma, no es suficiente para garantizar la ciberseguridad organizacional.

De ahí que, "la seguridad debe tenerse en cuenta en cada actividad de TI, pero tiene que satisfacer los requisitos y necesidades del negocio" (Bunker, 2012, p. 21). Además, describe tres grupos de control:

> controles estratégicos, tales como la alineación de negocios y la gobernanza; riesgo y cumplimiento; controles operacionales, incluida la seguridad física; Respaldo y manejo de incidentes y respuesta; y controles tácticos, como compilaciones seguras, antivirus e intrusión prevención.

[1] Entorno complejo que resulta de la interacción de las personas, *Software* y servicios a través de *Internet* por medio de dispositivos tecnológicos y redes conectados al mismo, que no existe en forma física alguna (ISO27032).

1.2 Características de los riesgos de ciberseguridad

El ciberespacio provee a nivel mundial diversas fuentes de oportunidades, para dotar de atributos de gran valor añadido a los procesos estratégicos, misionales, de apoyo y de evaluación y control, para que cada una de las organizaciones moderna identifiquen las fortalezas en materia de ciberseguridad para afrontar los desafíos de los ciberataques a las que están expuesta en su proceso de operación y permanencia en el mercado. Por consiguientes, el ciberespacio también es factor generador de amenazas a la sociedad en general, así como, a los sectores públicos como privado. En efecto, los beneficios que proporciona la información digital solo pueden lograrse cuando se impiden o minimizan toda una cadena de posibles riesgos y amenazas en cuanto a su integridad y confidencialidad, que van desde el fraude y el robo, hasta los ataques a la privacidad.

Bajo ese contexto, habitualmente los ciudadanos recepcionan información sobre nuevos ciberdelitos, los cuales algunas veces no están protegidos, tales como el hurto de información en formato electrónico; el "*phishing*", el robo de una clave de acceso a una cuenta desde una página falsa, así como, el secuestro de datos en el ciberespacio, que para efecto recuperarlos lleva consigo el pago de dinero ya sea en moneda física o moneda virtual "*bitcoin*". Es decir, que a partir de "la evolución de las TIC conlleva situaciones de riesgo que se van revelando día a día. Tecnologías emergentes habilitan el tratamiento de gran cantidad de datos, pero también habilitan su exposición" (Díaz, Molinari, Venosa, Macia, Lanfranco, & Sabolansky, 2018, p. 1056).

Las organizaciones en un entorno económico globalizado hoy en día se sienten más amenazadas en sus operaciones, toda vez que no establecen políticas para identificar, analizar, valorar y tratar los riesgos y vulnerabilidades cibernéticos. Tales amenazas, sino son tratadas a tiempos con medidas de control adecuadas, se verán abocadas frecuentemente a ataques cibernéticos, fraudes financieros y pérdida de información relevante para la toma oportuna de decisiones. Por lo tanto, han surgido métricas al respecto, que permiten calcular un puntaje asociado a un factor de riesgo o una vulnerabilidad. Así, el sistema de puntuación de vulnerabilidad común (CVSS, 2014), usa tres categorías de métricas: base, temporal y de entorno, las cuales, cada una de ellas, se estructuran a su vez de un conjunto de otras métricas.

De hecho, el aumento significativo del uso del ciberespacio por parte de los distintos sectores económico, político, educativo, social, científico, entre otros, ha permitido conocer las ventajas y desventajas para los grupos de interés en sus diferentes esferas. Por tanto, las características en

> el acceso, la transmisión de la información y bajo costo en la comunicación, se ha visto afectado por la existencia de riesgos que han puesto en cuestión la conveniencia de su uso en forma única por

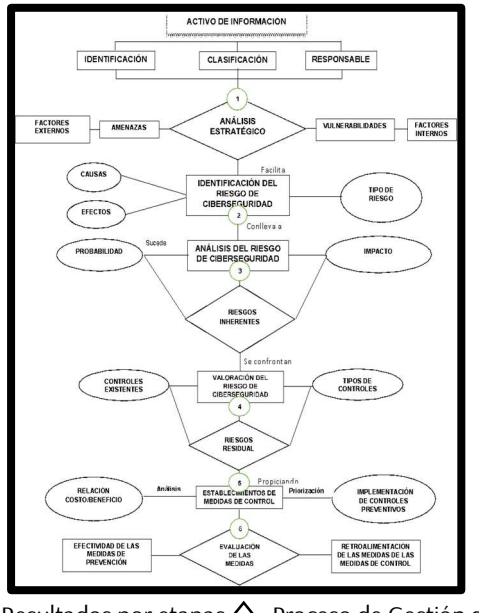
personas, organizaciones e instituciones (Sancho, 2017, p. 10).

Del análisis efectuado, se evidenció que, en el uso de TIC, coexisten factores de riesgos y vulnerabilidades cibernéticas que amenazan permanentemente las operaciones de las organizaciones en un entorno económico globalizado. En ese sentido, en cuanto a los sistemas de protección y control, la infraestructura de ciberseguridad y las competencias del talento humano, sino son abordadas desde un enfoque de control estratégico, de control operacional y de control táctico, podrían verse abocadas en consecuencias graves para su permanencia en el mercado de sus correspondientes organizaciones.

1.3 Medidas para la prevención de riesgos de ciberseguridad

Para establecer medidas de prevención para el control de los riesgos de ciberseguridad organizacional, es necesario que las organizaciones modernas tomen conciencias y gestionen de manera eficaz los mismos, mediante la adopción de políticas, procedimientos y controles preventivos.

Para efectos de implementar medidas de control para la prevención de los riesgos ciberseguridad organizacional, se sugiere un esquema de control de riesgo en ciberseguridad como el estipulado en la Figura 1.



Notación: Resultados por etapas ◇- Proceso de Gestión de Riesgos □
Figura 1. *Medidas de control de riesgos por Ciberseguridad.*
Fuente: Elaboración propia.

A partir de la Figura 1, como parte del producto de esta investigación, se describe y representa gráficamente el procedimiento sugerido en la subsección 3.1, sobre cómo las organizaciones pueden adoptar medidas de control de riesgos.

1.4 Auditoria forense: canalizando riesgos de ciberseguridad

Los riesgos que demanda el ciberespacio por la adopción de las TIC en las empresas modernas, las ha obligado en analizar las oportunidades de mejoras que existen en el mercado para la prevención de estos, de tal manera que no se vean involucradas en aspectos relacionados con fraudes financieros, delitos informáticos, actos de corrupción por manipulación de los sistemas de información u otros peligros que podría traer consecuencias graves para su operación. Por ello, para la prevención de los riesgos de ciberseguridad organizacional, es necesario analizar, además, los recursos de la auditoría forense y la gestión del conocimiento, como medidas claves para blindar a las organizaciones frentes a cualquier amenaza por ciberataques que las hagas vulnerables frente a la salvaguarda de las finanzas para cumplir con los planes estratégicos y financieros en el corto, mediano y largo plazo.

Por ello, la auditoría forense adquiere importancia con la evolución de los sistemas informáticos, debido al desarrollo de nuevos mecanismos utilizados por parte de las entidades para agilizar procesos organizacionales, presentando información confiable y oportuna a sus usuarios (Aros, Suárez y Rodríguez, 2016). Más aún, cuando esta herramienta, se convierte en un sistema de prevención y detección de operaciones dudosas o sospechosas que teniendo en cuenta las políticas y procedimientos adoptados por la administración, coadyuven en identificar y evaluar las amenazas y vulnerabilidades presentes por ciberataques, de tal forma que, revelen los delitos cometidos y el recaudo de las pruebas para su respectiva judicialización.

Bajo ese contexto, la investigación del cibercrimen y los delitos informáticos a partir de la auditoría forense requiere de habilidades especializadas de los investigadores, no solo por el incremento de la cantidad de datos digitales almacenados sino, por el desarrollo de nuevas técnicas de anonimato en el ciberespacio, lo cual les permite a los ciberdelincuentes, incrementar las probabilidades de impunidad (Toro-Álvarez, Jaimes y Ruiz, 2018). Por lo tanto, la auditoría forense como la gestión del conocimiento tiene mucho que aportar a las organizaciones, ya que son imprescindible para la prevención y control de las distintas formas del delito informático o el ciberdelito. Así pues, los expertos en seguridad tecnológica poseen la experiencia y las herramientas técnicas, mientras que los profesionales en procesos y sistemas de control industrial deben aportar su conocimiento de los sectores productivos, los procesos controlados y las limitaciones que el contexto impone a las soluciones específicas (Toro-Álvarez, Jaimes y Ruiz, 2018).

Por consiguiente, el panorama mundial en materia de seguridad cibernética y delito cibernético en el 2013 evalúa las tendencias más importantes en lo que respecta a las amenazas cibernéticas y a quienes afectan desde instituciones

gubernamentales, hasta empresas privadas y usuarios individuales (Aros, Suárez y Rodríguez, 2016).

A causa de lo anterior, a nivel internacional se han adoptados lineamientos para la prevención y judicialización de la ciberdelincuencia, con el fin de blindar las organizaciones dentro de este mundo globalizado, para lo cual una vez analizados los mismos, deben ser abordado con fundamento en el esquema de la Figura 2.

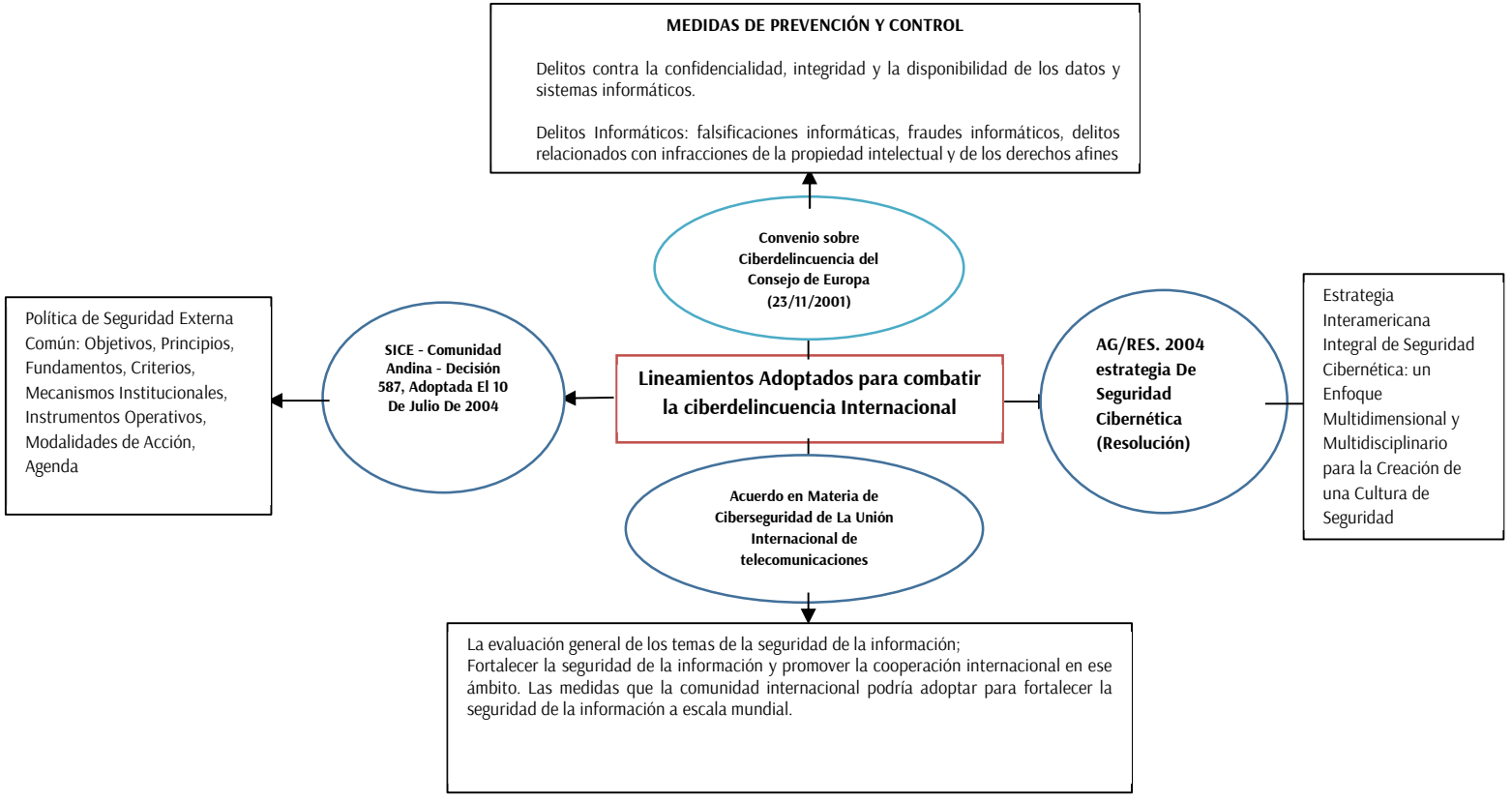


Figura 2. *Lineamientos para el aseguramiento de la información digital.*
Fuente: Elaboración Propia.

Bajo ese contexto, "la ontología de las disciplinas forenses digitales es un enfoque novedoso para organizar el conocimiento del dominio forense digital" (Karie, y Venter, 2014, p. 1231) y constituye la principal contribución de la auditoría forense en la gestión del conocimiento, no solo para la recolección de prueba pericial de un alto grado de legalidad, autenticidad y de aceptación científica, para el debido proceso en la cadena de custodia, lo que permitirá elevar el nivel de confianza de éstas en un proceso judicial (García-Holgado, García-Peñalvo y Cruz-Benito, 2015); también, como se gestiona el riesgo tanto en la infraestructura de ciberseguridad tecnológica como en los sistemas de protección y control de los procesos de negocio.

Incluso, de la calidad del control interno depende la calidad de los controles para la seguridad digital de la información y la previsión de riesgos de ciberseguridad organizacional, por lo que es necesario en las empresas modernas que pretendan resultados óptimos certeros, hacer evaluaciones periódicas a los mecanismos de control a través de la auditoria forense, como recursos de prevención para detectar debilidades, fraudes o actividades sospechosas. A partir de éstas, definir las medidas que se deben adoptar para mejorarlo, de tal forma que blinde a la entidad frente a cualquier riesgo de pérdida económica o de imagen, ocasionada por delitos informáticos, malversación de los recursos económicos y manejo inadecuado de los bienes.

No obstante, con el desarrollo de la complejidad de las operaciones en el ciberespacio dentro del mundo de los negocios, es necesario establecer controles preventivos efectivos (auditoria forense) que permitan garantizar un manejo adecuado de las finanzas de una organización, cerciorándose que dichas actividades se estén desarrollando acorde con las políticas, planes financieros e infraestructura de ciberseguridad que deben ser considerados dentro de los sistemas de planeación y control (ciberseguridad organizacional), como herramientas clave para pronosticar el nivel de operaciones o necesidades de fondos requeridos por la empresa para cumplir con su cometido social e institucional (Talento Humano).

De ahí que, Duarte (2015), describe que la auditoría forense debe ser objetiva, independiente y actualmente en la sociedad es necesaria para combatir la corrupción financiera, pública y privada. Por último, Paniagua (2018), examinó casos reales para apreciar de manera más práctica las consecuencias de este tipo de auditoría y su eficacia (efectividad y eficiencia), a la hora de reaccionar ante crímenes económicos. Como resultado se encontró que, en esta disciplina cada vez, se tiene más en cuenta como herramienta de lucha contra el fraude y además, muchas entidades públicas y privadas empiezan a aplicarla con mayor frecuencia.

Caamaño y Gil (2018), en la investigación realizada sobre Auditoría Forense y Ciberseguridad, Herramientas Clave para

Blindar las Empresas Modernas, concluyeron que la auditoría forense como recursos de prevención sirve además, como medio de prueba para los procesos judiciales que se adelanten en esta materia, como ocurrencia del fraude financiero, actos de corrupción y delitos informáticos que aunada a una adecuada Ciberseguridad organizacional, permitirá garantizar la seguridad de la confidencialidad de la información, la salvaguarda de los recursos físicos y financieros y por ende, la credibilidad y confianzas ante los clientes y partes interesadas.

1.5 Talento humano: competencias para prevenir los riesgos

La gestión del conocimiento en el Siglo XXI, se convierte en el activo intangible más poderoso de las organizaciones modernas, por cuanto, facilita la potencialización de las competencias del talento humano, como aspectos determinantes para generar capacidad instalada para afrontar los nuevos desafíos que demandan las dinámicas de los mercados en el contexto empresarial y financiero de la sociedad actual. Sin embargo, para que esto sea posible, es necesario establecer nuevos enfoques en la gestión del talento humano y alineado con las metas y objetivos en el direccionamiento estratégico de las empresas. Ello, con el fin de establecer políticas y procedimientos que faciliten la adquisición, distribución, almacenamiento, transformación y utilización de conocimiento, con el propósito de lograr ventajas competitivas en el mercado (Riesco, 2006; Barney, 1991; Dosi, Teece y Winter 1992).

Por otro lado, es necesario recalcar que la economía del conocimiento y la sociedad se caracteriza por la globalización económica, la aparición de los avances tecnológicos en varios dominios industriales y científicos y la primacía progresiva del conocimiento intensivo y tecnología basada en mercados industriales (Martín-de Castro, 2015). En este nuevo escenario competitivo, el conocimiento y los activos intelectuales se están convirtiendo en los nuevos factores clave de producción. Por ello, la gestión del conocimiento se convierte en una herramienta poderosa para la toma de decisiones en los distintos sectores económicos, político, sociales, entre otros, dentro de este mundo globalizado.

En este sentido, en la medida que las organizaciones modernas cuenten con profesionales y equipos de trabajos capacitados en el uso de las TIC y la seguridad de la información, les permitirá a las mismas, generar mayor capacidad instalada para afrontar con eficiencia y efectividad la ciberseguridad organizacional. De hecho, mediante el fortalecimiento de las competencias del talento humano, se optimizará el uso de los recursos tecnológicos y se minimizará el riesgo de daños y/o pérdida de información, sistemas y equipos por uso inadecuado. Por tal razón, la prevención de los riesgos de ciberseguridad, requiere para su adecuado tratamiento, de un conocimiento profundo de la ciberdelincuencia y de las competencias necesarias para trabajar en pos de su prevención e investigación, ya

sea en el ámbito policial o en el empresarial (Santos, Guisado y Morán, 2017).

En ese orden de ideas, la adopción de estándares internacionales y buenas prácticas para la prevención de riesgos, permitirá seleccionar profesionales con habilidades, capacidades y conocimientos para entender y administrar adecuadamente los sistemas de gestión de la ciberseguridad (Díaz, Molinari, Venosa, Macia, Lanfranco y Sabolansky, 2018). Por otra parte, se destacan avances en el desarrollo de las competencias para la gestión del conocimiento y la implantación de procesos, pero no se está haciendo gestión desde la estructuración de políticas, planes, programas y proyectos, falta avanzar en la apropiación y uso de prácticas y hay una deficiencia en la aplicación de herramientas tecnológicas para gestionar el conocimiento (Marulanda y López, 2013).

Bajo ese contexto, la gestión del conocimiento funge como medida de prevención de los riesgos de ciberseguridad organizacional, por cuanto, asume relevancia en la Sociedad del Conocimiento en tanto da cuenta del surgimiento de nuevas necesidades en las organizaciones que deben afrontar cotidianamente la complejidad y la contingencia de su entorno y para lo cual deben desarrollar la capacidad de "aprender a aprender" (Castro Chans, 2013). Por lo tanto, la gestión del talento y el conocimiento desempeñan un papel clave en la selección y el mantenimiento de la experiencia requerida (Fontenele y Sun, 2015). De ahí que, la gestión del conocimiento, se potencializa a partir de las competencias del talento humano requerida, que a través de la adopción e implementación de políticas y procedimientos establecidos, consolide un marco de referencia como medida de prevención y control que respondan a los nuevos desafíos de los riesgos de ciberseguridad generados por el uso de las TIC y se garantice la protección de las organizaciones modernas frente actividades fraudulentas o sospechosas que impidan del normal desarrollo de las operaciones y la salvaguarda de las finanzas para el cumplimiento de su cometido institucional.

2. Metodología

La investigación se enmarca en el paradigma cualitativo, por lo cual el investigador puede derivar resultados de su revisión bibliográfica y la subjetividad de su criterio (Hernández, Fernández y Baptista, 2010). A la vez, se encuadra en el estudio de tipo exploratoria, descriptiva y documental, con un diseño bibliográfico, ya que se recolecta información de fuentes primarias ubicadas en texto y material digital.

En ese sentido, este artículo recopila resultados de la investigación referente los riesgos de ciberseguridad organizacional, que a partir de las medidas de prevención y control de la auditoria forense y la gestión del conocimiento se adopten las mismas para la prevención de riesgos de fraude financiero, delitos informáticos, actos de corrupción y de seguridad, a los que se

encuentran expuestas las organizaciones actualmente a nivel mundial. De lo anterior, se aplicaron los siguientes procedimientos:

1) A nivel de los riesgos de ciberseguridad, se sintetizaron métricas del sistema de puntuación de vulnerabilidad común (CVSS, 2014), para priorizar medidas de seguridad.
2) Para evitar ataques cibernéticos a los activos de información, se propone un procedimiento para que las organizaciones modernas adopten e implementen el mismo.
3) Luego de revisar, las posiciones para combatir la ciberdelincuencia internacional, se sugiere una representación que ilustra cómo se relacionan esta terminología.

3. Resultados obtenidos

Del análisis de los hechos observados, a través de la revisión bibliográfica utilizada, se evidenció que a nivel mundial han existido casos por falta de medidas efectivas de ciberseguridad organizacional. En ese sentido, se han materializado los riesgos y vulnerabilidades cibernéticos en el contexto de la gobernanza, la infraestructura tecnológica, la planeación estratégica y las competencias del talento humano, que han impactado a la sociedad, la economía y las organizaciones tanto del sector público como privado. Concretamente, se han producido desfalcos, fraudes, delitos informáticos, entre otros que, si no son judicializados a tiempo, seguirán aumentado dicho problema, y por ende, la desestabilización económica dentro de este mundo globalizado.

Por otra parte, se evidenció que la auditoría forense es un sistema de prevención y control expedito, para la detección de operaciones fraudulentas o sospechosas en las empresas modernas el uso de las TIC, que integrada a una sólida gestión del conocimiento, se garantizará la efectividad y eficiencia de las pruebas ante la investigación de crímenes económicos y delitos cibernéticos para la defensa de los procesos judiciales, así como, la ciberseguridad organizacional de las finanzas para atender los planes estratégicos y financieros de largo plazo, según la Figura 3.

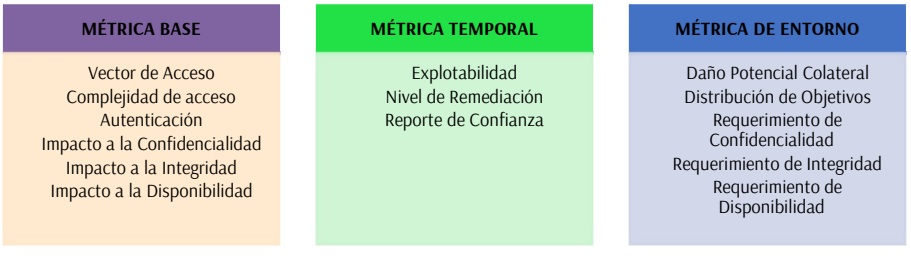


Figura 3. *Métricas para medir vulnerabilidades.*
Fuente: Adaptado de Mendoza (2014).

En este sentido, la ciberseguridad organizacional debe concebirse como un sistema integrado, de tal forma, que sus componentes al interrelacionarse entre sí, con la gestión del conocimiento y la auditoría forense, se blinde a las organizaciones modernas, mediante la exigencias y puesta en práctica de valores y principios corporativos, propios del buen gobierno, así como, de política, planes y programas que fortalezcan las competencias del talento humano, para la prevención y control de los riesgos ocasionados por ciberataques o actividades sospechosas que atenten contra la infraestructura tecnológica e impida la toma oportuna de decisiones en la ejecución de los planes estratégico para los fines esenciales de la sociedad, el Estado, los clientes y las partes interesadas.

3.1 Procedimiento

En primer lugar, hacer los análisis estratégicos que permita la identificación, clasificación y de los responsables de los activos de información sujetos hacer impactados por estos problemas. De hecho, se deberá adoptar y estandarizar políticas para la gestión de los riesgos a nivel institucional, para que el proceso sea más expedito y genere los impactos requeridos para la prevención de la materialización de éstos. En este proceso, se deben identificar los factores externos (amenazas) y los factores internos (vulnerabilidades) en cuanto a la infraestructura de ciberseguridad, los sistemas de protección y control y de talento humano, con el fin de determinar de manera efectiva las causas que podrían dar lugar a la identificación de los riesgos.

En segundo lugar, se realiza el proceso de identificación de los riesgos de ciberseguridad organizacional, caracterizando el riesgo en cuanto sus causas y posibles consecuencias que podrían traer para las organizaciones modernas.

En tercer lugar, se procede al análisis de los riesgos de ciberseguridad organizacional, examinando la probabilidad e impacto de ocurrencia, para establecer el nivel de riesgo inherente a que están expuesto los procesos de las empresas.

En cuarto lugar, el nivel de riesgo inherente es sometido a los controles existentes adoptados por las organizaciones, a través de la valoración de los riesgos de ciberseguridad, conllevando a establecer el nivel de riesgos residual, a los cuales, la alta dirección y responsables de los procesos, deberán establecer medidas de prevención adecuadas para atacar las causas e impactos que generan los mismos.

En quinto lugar, para el establecimiento de medidas de prevención y control es fundamental que se realice un análisis de costo/beneficio sobre las acciones preventivas a implementar para disminuir el impacto o probabilidad de los riesgos de ciberseguridad, que si llegaren a materializarse no afecte como un todo, la operación.

En último lugar, se encuentra la evaluación de las medidas de prevención implementadas para los riesgos de ciberseguridad

organizacional, las cuales, a través del monitoreo y seguimiento realizado por el responsable del proceso establecer el nivel de avance de implementación.

En concreto, la evaluación independiente a través de la auditoria forense, para establecer el nivel de eficiencia, y efectividad (eficacia) de las medidas implementadas. Por último, el Comité de Gestión de Riesgos conforme a los informes presentados por el monitoreo y seguimiento y de la evaluación independiente, tomar decisiones oportunas sobre las medidas de ciberseguridad adoptadas para la prevención de los riesgos.

Finalmente la gestión del conocimiento se constituye en un soporte esencial para la ciberseguridad de las organizaciones modernas, por cuanto, provee las competencias necesarias del talento humano para implantar sistemas de prevención y control, que mediante políticas, procedimientos, planes y programas, se garantice la prevención de los riesgos por actividades sospechosas o fraudulentas, que armonizada con la auditoría forense, se consolidaría una efectiva gestión integral de la seguridad informática a través del uso de las TIC.

En síntesis, para garantizar la prevención de los riesgos de ciberseguridad organizacional, se propone que desde la auditoría forense aunado con la gestión del conocimiento (talento humano), se adopten mecanismos de control interno y protección para garantizar la eficacia de las operaciones.

En ese sentido, se representa entonces en la Figura 3, como un resultado parcial, los lineamientos para el aseguramiento de la información digital, en términos de normativas y regulaciones recientes a nivel internacional.

Conclusiones

Analizados y discutidos los resultados obtenidos en la presente investigación, se procedió a la emisión de conclusiones en atención a los objetivos propuestos:

- En cuanto al primer objetivo específico, se identificaron las características de los riesgos de ciberseguridad organizacional, lo cual, facilitará a los responsables de los procesos estratégicos, misionales, de apoyo y de evaluación y control, precisar las medidas de seguridad que podrían ser factible para contrarrestar el impacto de la materialización de los mismos.
- Asimismo, con relación al segundo objetivo específico, se establecieron medidas de control que permiten garantizar la ciberseguridad organizacional, mediante el desarrollo de las etapas o fases definidas en el esquema de la Figura 2 que, armonizado con la gestión del conocimiento y la auditoría forense, se blinden a las empresas modernas frente a cualquier ciberataque.
- También en cuanto al tercer objetivo específico, se analizaron las competencias del talento humano para administración de la ciberseguridad organizacional, determinándose que la gestión del conocimiento es la principal fuente que provee los perfiles idóneos que, al conjugarse con la auditoría forense, se

garantiza la capacidad instalada para la efectiva implementación de las medidas de control de prevención frente al nivel de exposición de los riesgos en los procesos de la organización.

- Por último, en relación con el objetivo de valor agregado de la investigación, se formularon lineamientos para el mejoramiento de la ciberseguridad organizacional que, a partir de la gestión del conocimiento del talento humano y la auditoría forense, los responsables de los procesos sujetos a riesgos por ciberataques, implementen políticas y procedimientos para prevenir la materialización de los mismos.

Referencias

Aros, l. H., Suárez, j. A. C., y Rodríguez, j. A. V. (2016). Riesgos presentes en los ciberataques: un análisis a partir de herramientas de auditoría forense. Pensamiento Republicano, (3).

ASOBANCARIA, Semana Económica 2018 – Edición 1133, Consultado el 14 de marzo de 2019 en http://www.asobancaria.com/2018/04/23/edicion-1133/.

Barney, J., Firm Resources and sustained competitive advantage, Journal of management: 17(1), 99-120 (1991), http://business.illinois.edu/josephm/BA545_Fall%202011/S10/Barney%20%281991%29.pdf. Consultado: 13 de marzo (2019).

Bunker, G. (2012). La tecnología no es suficiente: tener una visión holística para asegurar la información. Informe Técnico de Seguridad de la Información, 17 (1-2), 19-25.

Caamaño F., E.E y Gil H., R.J. (2018). Auditoría Forense y Ciberseguridad, Herramientas Clave para Blindar las Empresas Modernas. Revista Contabilidad Impuestos Finanzas ISSN 2422-2372. Universidad Popular del Cesar – Seccional Aguachica-Colombia.

Carrasco, Ó. N., y Puerta, A. V. (2013). Una visión global de la ciberseguridad de los sistemas de control. Revista SIC: ciberseguridad, seguridad de la información y privacidad, (106), 52-55.

Castro Chans, B. (2013). Las interacciones comunicativas en los procesos de gestión de conocimiento en la universidad. Question, 1.

Díaz, F. J., Molinari, L. H., Venosa, P., Macia, N., Lanfranco, E. F., y Sabolansky, A. J. (2018). Investigación en ciberseguridad: un enfoque integrado para la formación de recursos de alto grado de especialización. In XX Workshop de Investigadores en Ciencias de la Computación (WICC 2018, Universidad Nacional del Nordeste).

Dosi, G., D., Teece y S. Winter, Toward a theory of corporate coherence: preliminary remarks, En Technology and Enterprise in a Historical Perspective, Oxford : Clarendon Press ; New York: Oxford University Press, USA (1992), http://trove.nla.gov.au/work/20422348?versionId=24154413. Consultado: 13 de marzo (2019).

Duarte, G. A. (2015). Importancia de la Auditoría Forense en las

organizaciones del sector comercial en Colombia.

Fontenele, M. P., y Sun, L. (2015, junio). Descubrimiento del talento para la seguridad cibernética: una perspectiva organizativa. En 2015, la Conferencia Internacional sobre Concienciación, Análisis y Evaluación de Datos Cibernéticos (CyberSA) (pp. 1-4). IEEE

García-Holgado, A., García-Peñalvo, F. J., y Cruz-Benito, J. (2015). Análisis comparativo de la gestión del conocimiento en la administración pública española.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2010). Metodología de la investigación.

Jirasek, V. (2012). Aplicación práctica de modelos de seguridad de la información. Informe técnico de seguridad de la información, 17 (1-2), 1-8.

Karie, N. M., y Venter, H. S. (2014). Hacia una ontología general para las disciplinas forenses digitales. Revista de ciencias forenses, 59 (5), 1231-1241.

Leiva, E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en enfoque Top-Down desde una visión global a una visión local. Revista Latinoamericana de Ingeniería de *Software*, 3(4), 161-176.

López, M., Hernández, A., & Marulanda, C. E. (2014). Procesos y prácticas de gestión del conocimiento en cadenas productivas de Colombia. Información tecnológica, 25(3), 125-134.

Martín-de Castro, G. (2015). Knowledge management and innovation in knowledge-based and high-tech industrial markets: The role of openness and absorptive capacity. Industrial Marketing Management, 47, 143-146.

Marulanda Echeverry, C. E., y López Trujillo, M. (2013). La gestión del conocimiento en las PYMES de Colombia. Revista Virtual Universidad Católica del Norte, 1(38), 158-170.

Mendoza, M.A. (2014). Vulnerabilidades: ¿qué es CVSS y cómo utilizarlo? WeLiveSecurity, México. Recuperado de https://www.welivesecurity.com/la-es/2014/08/04/vulnerabilidades-que-es-cvss-como-utilizarlo/

Paniagua Artazkoz, A. (2018). La auditoría forense como herramienta de prevención y detección del fraude.

Riesco, M., El negocio es el conocimiento, Ediciones Díaz de Santos, Madrid, España (2006).

Sancho, C. (2017). Ciberseguridad. Presentación del dossier/Cybersecurity. Introducción to Dossier. URVIO-Revista Latinoamericana de Estudios de Seguridad, (20), 8-15.

Santiago, E. J., y Allende, J. S. (2017). Riesgos de ciberseguridad en las empresas. Tecnología y desarrollo, (15), 10.

Santos, C. P., Guisado, Á. C., y Morán, J. J. D. (2017). El fenómeno de la ciberdelincuencia en España: La propuesta de la Universidad Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito. Revista Policía y Seguridad Pública, 7(1), 237-270.

Tisdale, S. M. (2015). Ciberseguridad: desafíos desde una perspectiva de sistemas, complejidad, gestión del conocimiento y inteligencia empresarial. Problemas en los sistemas de información, 16 (3).

Toro-Álvarez, M. M., Jaimes, W. D. P., & Ruiz, E. O. (2018). Fundamentos de la investigación forense en ambientes informáticos.

Yahia, N., Mokhtar, S. A., & Ahmed, A. (2012). Automatic generation of OWL ontology from XML data source. arXiv preprint arXiv:1206.0570.