Sistemas de gestión de seguridad de la información para empresas KPO: una aproximación*[1]

Computer security management systems for KPO companies: an approximation

Sistemas de gerenciamento de segurança da informação para empresas KPO: uma aproximação

Eduar MORALES OSORIO[2], Marcelo LÓPEZ TRUJILLO[3]

Recibo: 02.08.2017 – Aprobación: 20.03.2018

Resumen: *La información es considerada el activo más importante de una organización, por lo cual se requieren mecanismos que garanticen la integridad, confiabilidad y disponibilidad de ella. En el caso de las empresas KPO (Knowledge Process Outsourcing) que manejan activos de información cruciales para sus clientes, deben garantizar un alto nivel de confianza, surgiendo la necesidad de*

* **Modelo para la citación de este artículo / Template for citation of this article / Modelo para a citação deste artigo:**
MORALES OSORIO, Eduar & LÓPEZ TRUJILLO, Marcelo (2017). Sistemas de gestión de seguridad de la información para empresas KPO: una aproximación. En: Ventana Informática No. 37 (jul-dic). Manizales (Colombia): Facultad de Ciencias e Ingeniería, Universidad de Manizales. p. 73-87. ISSN: 0123-9678

1 Artículo de reflexión / Reflection Article / Artigo de reflexão
Proyecto / Project / Projeto: Estudio y análisis de los sistemas de gestión de seguridad informática para empresas KPO (Trabajo de grado) / Study and analysis of computer security management systems for KPO companies (Degree work) / Estudo e análise de sistemas de gerenciamento de segurança de computadores para empresas de KPO (Trabalho de grado)
Periodo / Period / Período: 27/11/2015 - 24/11/2016
Institución / Institution / Instituição: Universidad Nacional de Colombia (Manizales, Caldas, Colombia).

2 Estudiante de Administración de Sistemas Informáticos / Student of Computer Systems Administration / Estudante de Administração de Sistemas de Computação, Universidad Nacional de Colombia (Manizales, Caldas, Colombia). emoraleso@unal.edu.co

3 Doctor en Ingeniería informática / Doctor in Computer Engineering / Doutor em Engenharia de Computação. Catedrático asociado / Associate professor / Professor associado, Universidad Nacional de Colombia (Manizales, Caldas, Colombia), Profesor titular / Titular professor / Titular professor / Professor titular, Universidad de Caldas (Manizales, Caldas, Colombia). mlopeztr@unal.edu.co. https://orcid.org/0000-0003-0668-1292
Proyecto / Project / Projeto: Estudio y análisis de los sistemas de gestión de seguridad informática para empresas KPO (Trabajo de grado) / Study and analysis of computer security management systems for KPO companies (Degree work) / Estudo e análise de sistemas de gerenciamento de segurança de computadores para empresas de KPO (Trabalho de grado)
Periodo / Period / Período: 27/11/2015 - 24/11/2016
Institución / Institution / Instituição: Universidad Nacional de Colombia (Manizales, Caldas, Colombia).

analizar y entender cómo se debe proteger la información de terceros, qué mecanismos y herramientas se implementan y de qué manera un sistema de gestión de seguridad de la información aporta al mejoramiento de la protección de la información. El artículo se divide en cuatro segmentos: el primero establece un contexto de la temática, el segundo revisa antecedentes, en el tercero se propone un referente conceptual con sus recomendaciones y, finalmente, se plantean las conclusiones y trabajos futuros.

Palabras clave: *Seguridad de la información, gestión del riesgo, políticas de seguridad, Knowledge process Outsourcing.*

Abstract: *Information is considered the most important asset of an organization, which requires mechanisms that guarantee the integrity, reliability and availability of it. In the case of KPO (Knowledge Process Outsourcing) companies that handle crucial information assets for their clients, they must guarantee a high level of trust, with the need to analyze and understand how third-party information should be protected, what mechanisms and tools they are implemented and in what way an information security management system contributes to the improvement of information protection. The article is divided into four segments: the first establishes a context of the subject, the second reviews background, the third proposes a conceptual reference with its recommendations and, finally, the conclusions and future works are presented.*

Keywords: *Computer security, risk management, security policies, Knowledge process Outsourcing*

Resumo: *A informação é considerada o bem mais importante de uma organização, que exige mecanismos que garantam a integridade, confiabilidade e disponibilidade. No caso das empresas KPO (Knowledge Process Outsourcing) que lidam com ativos de informações cruciais para seus clientes, elas devem garantir um alto nível de confiança, com a necessidade de analisar e entender como as informações de terceiros devem ser protegidas, quais mecanismos e ferramentas eles são implementados e de que forma um sistema de gerenciamento de segurança da informação contribui para a melhoria da proteção da informação. O artigo é dividido em quatro segmentos: o primeiro estabelece um contexto do assunto, o segundo plano de fundo, o terceiro propõe uma referência conceitual com suas*

recomendações e, finalmente, são apresentadas as conclusões e as obras futuras.

Palavras-chave: *segurança da informação, gerenciamento de risco, políticas de segurança, processo de conhecimento Outsourcing.*

Introducción

Con la evolución de la sociedad del conocimiento, la globalización económica y la emergencia de la economía del conocimiento, aparecen nuevas formas de relaciones productivas que disminuyen la rigidez laboral; «*un caso concreto se evidencia en las actividades de outsourcing*[4] *en empresas que optan por deslocalizar algunos procesos y generar transferencia de empleos a lugares donde las condiciones de contratación son menos rígidas; esta modalidad se conoce como outsourcing por offshoring*» (Castro & Serna, 2016, 206). De acuerdo con García (2017, 8), «*la tercerización de servicios existe básicamente por dos razones: a) las empresas pueden disminuir sus costos de operación al contratar quién haga determinadas tareas por ellos y b) por que quien provee los servicios le puede brindar una ventaja competitiva*», que puede darse desde tres modalidades: BPO, ITO y KPO.

> «*BPO: Tercerización de procesos de negocio o Business Process Outsourcing. Se entiende como la delegación de uno o más procesos de negocio intensivos en el uso de tecnologías de la información y comunicaciones a un proveedor externo, quien a su vez posee, administra y gerencia los procesos seleccionados, basado en métricas definidas y medibles.* (…)
>
> *ITO: Tercerización de servicios de tecnología de la información, o Information Technology Outsourcing. Definido como la delegación a un proveedor externo de uno o más procesos de negocio relacionados con las tecnologías de información, sistemas de información y plataformas tecnológicas, cuyo modelo de prestación esté basado en la modalidad del cobro por servicio*» (García, 2017, 9-10).

La tercera modalidad, interés del presente artículo, corresponde a la industria de externalización de servicios de procesos de conocimiento

4 «*El contrato Outsourcing es conocido también como descentralización productiva, externalización del negocio, externalización de actividades, tercerización de la información, subcontratación o contratación de servicios externos entre otros*» (Ardon & Escobar, 2016, 36).

(KPO: *Knowledge Process Outsourcing*), que para Ramalingam, Archana Bai & Vimala (2007, 1070), «*en un nivel básico, KPO se refiere a los procesos intensivos del negocio que requiere experiencia basada en el dominio especializado*», en como lo cita García (2017, 10) «*la delegación a un proveedor externo de una o más actividades o procesos de negocio intensivos en manejo de conocimiento y cuyo modelo de negocios esté basado en el cobro por demanda de acuerdo con el servicio prestado*[5]».

> «*Además de los beneficios que se generan con la tercerización, también existen riesgos y problemas, como por ejemplo la pérdida de control y dependencia al proveedor. Al respecto, Mcfarlan y Nolan (como se citó en Valero & Salvador, 2008, p. 667) consideran que la relación entre la organización y el proveedor de outsourcing debe ser como de socios; es decir, aunque se relacionen, debe ser independiente una de otra. Por esta razón, la organización debe conocer los recursos con los cuales cuenta para el desarrollo de su actividad económica (Acevedo, 2014) y, al mismo tiempo, saber cuáles son los factores necesarios que la llevan a ser más productiva. Así le será más fácil conocer la actividad a subcontratar, la cual dependerá de un tercero para su óptimo desarrollo, lo que la hace vulnerable por los riesgos propios del proveedor*» (Alarcón, Gómez & Stellian, 2016, 103).

Las características mismas de la información que maneja esta industria, impone que la seguridad informática[6] se convierta en un aspecto fundamental en su quehacer, puesto que, como lo asegura Páez (2017, 24), al ser la información un recurso o activo esencial en una organización y en su operación, necesita ser protegida adecuadamente, especialmente en el ambiente comercial cada vez más interconectado y por lo tanto expuesta a una variedad creciente de amenazas y vulnerabilidades.

5 Entre los servicios de tercerización pueden listarse: investigación y desarrollo, telemedicina y salud, ingenierías, servicios legales, diseño de video juegos, diseño gráfico, análisis financiero y de riesgos, investigación de mercados y educación remota.

6 Entendida «*como un conjunto de mecanismos de prevención, detección y corrección, dirigidos a la protección de la confidencialidad, integridad y disponibilidad de los recursos informáticos* (…). *En los últimos años, la vigencia de los temas referidos a seguridad informática comenzó a extenderse a otras áreas, tal es así que trascendió las fronteras de la informática propiamente dicha, elevó de alguna manera su horizonte de responsabilidad y constituyó el nuevo concepto de seguridad de la información. Esto se basa en que la información va mucho más allá de la netamente procesada por equipos informáticos y sistemas, es decir, también abarca aquello que pensamos, que está escrito en un papel que decimos, etcétera)*» (Benchimol, 2011, 12).

Así, ya que las empresas KPO[7] prestan un servicio especializado a otras organizaciones, es imprescindible que entre ambas exista un alto grado de confianza al tratar con temas que aportan una mejora en la cadena de valor, tienen la obligación natural de asegurar la información que maneja, garantizando sus condiciones de integridad, confidencialidad, disponibilidad e irrefutabilidad.

1. Empresas KPO

Las empresas KPO se caracterizan como fuente primaria de información y conocimiento o por utilizar el conocimiento para producir servicios intermedios para el proceso de producción de los clientes, es decir, señalan Laumer, Blinn & Eckhardt (2012, 3828), son servicios que proveen insumos intensivos de conocimiento a los procesos de negocio de otras organizaciones.

Al hablar de empresas KPO debe considerarse, de acuerdo con Curie, Michell & Abanishe (2008, 95), que un proceso de conocimiento es una secuencia de actividades intelectuales que involucran el análisis, reconocimiento de patrones, planificación y criterio, lo que convierte la entrada (*input*) de un proceso poco y pobremente estructurado, en un producto (*output*) a menudo original. Debido a que tales procesos contienen diferentes niveles de conocimiento, se requieren diversos niveles y capacidades para explotar al máximo el conocimiento inherente al proceso, que conllevan características de un proceso de conocimiento: - que sea analítico, - que permita la toma de decisiones complejas y profesionales, - que involucre dominio del conocimiento amplio y complejo, - que requiera de personal altamente y profesionalmente calificado, - que sea un proceso o recurso no estructurado y que se automatice fácilmente, o - que sea creativo y dinámico con un propósito.

En el marco de la tercerización, es indispensable tener presente que «*como en todo contrato bilateral, ya sea de naturaleza civil o mercantil, existe una reciprocidad de derechos y obligaciones entre las partes*

7 «*El sector KPO, caracterizado por ser el sector de mayores tasas de crecimiento a nivel global, tiene una taxonomía constituida por 9 subsectores, la gran mayoría de ellos incipientes en cuanto a su propia comprensión y proyección. Muchos de los subsectores de servicios involucrados, no perciben aún que sus servicios sean KPO a pesar que su modelo de negocio en varias de sus líneas, son marcadamente de tercerización. Como ejemplo, el sector de servicios legales no considera regularmente que sus contratos con grandes clientes locales o internacionales sean KPO a pesar de contratarlos de manera indefinida y de tener responsabilidad y delegación de múltiples procesos de conocimiento (ej: contratación, demandas, laboral, etc.)*» (Programa de Transformación Productiva, 2014, 15).

contratantes. Y para el contrato Outsourcing no es la excepción, ya que (…)*, existen dos sujetos intervinientes en el mismo, los cuales son por un lado la empresa cliente y por otro la Outsourcer*» (Ardon & Escobar, 2016, 44), para así disminuir los riesgos (de propiedad intelectual, confidencialidad, reputación, entre otros) que puedan presentarse a partir de la relación contractual y que son especialmente relevantes para las empresas que operan con datos sensibles e información acerca de clientes y proveedores. Por ello, en todo contrato de *outsourcing*, señalan Curie, Michell & Abanishe (2008, 100), la amenaza de infracción de la propiedad intelectual es delicada, por lo que debe ser considerada antes de firmarlo. Es aquí donde se genera la necesidad de proteger la información y la seguridad informática toma alta relevancia, ya que su propósito, según Fazlida & Said (2015, 244), es proteger y preservar la confidencialidad, integridad y disponibilidad de la información.

> «*Es esencial que una organización identifique sus requerimientos de seguridad.* (…) *1. Evaluar los Riesgos de la Organización, mientras se tienen en cuenta la estrategia de negocio global de la organización y sus objetivos. A través de una valoración de riesgo, se identifican amenazas a los recursos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se estima el impacto potencial. 2. Requerimientos legales, estatutarios, reguladores y contractuales que la organización, sus socios comerciales, contratistas, y proveedores de servicios tienen que satisfacer y el ambiente socio-cultural. 3. Conjunto particular de principios, objetivos y requerimientos comerciales para la información que se procesa que una organización ha desarrollado para apoyar sus funcionamientos*» (Páez, 2017, 27-28)

Sobre la relación empresas KPO y seguridad de la información, se encuentran algunos casos reportados en la literatura científica:

- Longfei et al. (2013, 147-150) enfatizan en la necesidad de acuerdos de confidencialidad entre los proveedores del servicio y sus clientes, ya que se les confía el manejo de procesos del negocio relacionados con el trabajo intelectual, investigación, innovación y desarrollo. La necesidad de proteger los datos y la información de los clientes es fundamental, lo que exige una adecuada gestión de riesgos, partiendo de la identificación de riesgos, como paso fundamental, considerando los riesgos de exponer secretos comerciales, de la posesión de propiedad intelectual, y de infringir la propiedad intelectual.

- Jidiga & Sammulal (2013) señalan que las personas no son conscientes de las amenazas tecnológicas existentes, lo cual se agrava debido a que continuamente aparecen nuevos técnicas de ataques informáticos, especialmente del tipo DoS (*Denial of Service*), *phising*, *spyware*, *malware* y robo de información. Por ello proponen un paradigma de seguridad de 3-LSP.
- Moyo, Abdullah & Nienaver (2013, 1-6) realizan la evaluación de la administración del riesgo para la seguridad informática en dos escuelas secundarias de Sudáfrica, y recomiendan el método OCTAVE para suplir las falencias encontradas, ya que identifica prioridades y gestiona los riesgos de la seguridad de la información, mediante la adaptación a cuatro pasos: Identificar los activos críticos del sistema de información, Identificar amenazas sobre estos activos del sistema de información, Identificar vulnerabilidades en las instalaciones de computo y Evaluación del riesgo, desarrollo e implementación de estrategias para tratar el riesgo.
- Nancylia et al. (2014) buscan diseñar un mecanismo que permita la evaluación y medición del alcance de los sistema de gestión de seguridad de la información basados en estándares ISO (ISO/IEC 27004: 2009 y la ISO/IEC 27004: 2013, enfocadas en la evaluación y medición de la seguridad de la información).

Una revisión de los elementos anteriormente nombrados se pueden encontrar aspectos en común: - la información es un activo esencial y que tiene un valor dentro de las organizaciones, ya sean empresas, escuelas o cualquier otro tipo de organización que cuente con sistemas informáticos, por tal razón es un activo que se debe proteger, - la implementación de métodos para la gestión del riesgo, - la necesidad de crear consciencia frente a la importancia de la seguridad informática en las organizaciones, para así implementar mecanismos que permitan prever y mitigar los eventos de seguridad que amenazan los activos informáticos de las organizaciones.

2. Propuesta de gestión de seguridad de la información en empresas KPO

La propuesta se basa en la NTC-ISO-IEC 27001 (Icontec, 2013) que especifica los requisitos para establecer, implementar, operar, revisar y mejorar un sistema de gestión de seguridad de la información, SGSI, con un enfoque basado en procesos, es decir, en la identificación e

interacción de los procesos. Además se utiliza la metodología PHVA (Planificar, Hacer, Verificar, Actuar) dentro de la estructura de procesos del SGSI.

Con este modelo se realiza una modificación a la metodología PHVA, donde se proponen implementar mecanismos de prevención, detección y corrección dirigidos a la protección de los recursos informáticos en el contexto de las empresas KPO. Presenta un enfoque en cascada, donde el inicio de cada etapa corresponde al final de la etapa anterior:

- Etapa de diagnóstico: realiza un diagnóstico inicial y comprende el estado en el que se encuentra la empresa, considerando las políticas de la empresa, los acuerdos de confidencialidad con los clientes, los procesos de negocio, plataformas de hardware y software utilizadas por la empresa, la identificación de activos e identificación del riesgo en los activos informáticos[8].
- Etapa de arranque: se implementan mecanismos preventivos, como los controles para mitigar los riesgos informáticos.
- Etapa de comprobación: se implementan mecanismos de detección sobre los controles propuestos, para determinar si realmente son acordes con los riesgos encontrados, se debe realizar un seguimiento del estado del activo y los posibles eventos de seguridad que pueden ocurrir y proponer un plan de choque.
- Etapa de reajuste: se implementan mecanismos de corrección, verifica si ha ocurrido algún evento de seguridad para implementar el plan de choque correspondiente, compara el estado inicial de la empresa y el estado de la empresa en la etapa actual para determinar cambios organizacionales (de ser así, se debe implementar de nuevo el modelo, de lo contrario se pasará por las primeras dos etapas sin implementar nuevos mecanismos y se continuará haciendo un seguimiento en la etapa de comprobación).

Los requisitos de seguridad están determinados por las variables que tienen un alcance directo sobre la información, es decir, los activos informáticos, que en el caso de las empresas KPO, tienen una

8 Los activos informáticos son los recursos utilizados en la generación, procesamiento, almacenamiento o transmisión de la información, con un alcance directo sobre la información, lo que los convierte en requisitos de seguridad. Para realizar su identificación se recomienda la metodología Magerit (2012, 23), que los divide en las siguientes categorías: «- *Datos que materializan la información. - Servicios auxiliares que se necesitan para poder organizar el sistema. - Las aplicaciones informáticas (software) que permiten manejar los datos. - Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios. - Los soportes de información que son dispositivos de almacenamiento de datos. - El equipamiento auxiliar que complementa el material informático. - Las redes de comunicaciones que permiten intercambiar datos. - Las instalaciones que acogen equipos informáticos y de comunicaciones. - Las personas que explotan u operan todos los elementos anteriormente citados*».

característica especial ya generalmente son intangibles y representan conocimiento, por ejemplo, *Know-How*, Patentes, Propiedad intelectual y secretos comerciales (organizacionales). El primer paso para asegurarlos es realizar una identificación de los mismos. La importancia de realizar su inventario está en que la empresa tiene un control sobre la existencia de estos activos y así, se es consciente sobre los riesgos y vulnerabilidades que pueden presentar; además de su adecuada identificación, que es el inicio de cualquier metodología de análisis y gestión del riesgo.

Después de tener dicho inventario, se realiza el análisis, evaluación y tratamiento del riesgo. La metodología que más se adapta para el contexto de las empresas KPO es MAGERIT (Ministerio de Hacienda y Administraciones Públicas, 2012, 9), ya que permite considerar los pilares de la seguridad informática (Confidencialidad, Integridad y Disponibilidad), al momento de valorar los activos informáticos. Debido a que el activo esencial en las empresas KPO son los datos y la información, no se les puede dar una valoración cuantitativa, por lo cual se analizan análisis mediante tablas, con una escala para los activos, la magnitud del impacto y la magnitud del riesgo, con las categorías *MB: muy bajo, B: bajo, M: medio, A: alto y MA: muy alto*.

La estimación del Impacto (Tabla 1), usa la degradación, indicando qué tan perjudicado resultaría el valor del activo en el supuesto caso de un incidente. Antes de estimar el riesgo, se establecen las escalas cualitativas para el impacto, probabilidad y riesgo (Tabla 2), utilizadas en el modelo.

Tabla 1. Estimación del impacto

Impacto		Degradación		
		1%	10%	100%
Valor	**MA**	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Tabla 2. Escalas cualitativas de impacto, probabilidad y riesgo

Impacto	Probabilidad	Riesgo
MA: Muy alto	MA: Prácticamente seguro	MA: Crítico
A: Alto	A: Probable	A: Importante
M: Medio	M: Posible	M: Apreciable
B: Bajo	B: Poco probable	B: Bajo
MB: Muy bajo	MB: Muy raro	MB: Despreciable

Con base en ellas puede determinarse el riesgo potencial (Figura 1), definido por Ministerio de Hacienda y Administraciones Públicas (2012, 29-30), como la medida del daño probable sobre un sistema o un activo, que puede determinarse en función de la probabilidad y el impacto mediante zonas específicas: - Zona 1: ubicada en el extremo superior derecho, son los riesgos más probables y de más fuerte impacto, - Zona 2: en el centro del recuadro, son los riesgos con un gran rango de situaciones que son improbables y de impacto medio o incluso situaciones proco probables y de impacto bajo o muy bajo, - Zona 3: ubicada en el extremo inferior izquierdo, son los riesgos improbables y de bajo impacto, y - Zona 4: localizada en la esquina superior izquierda, son los riesgos improbables pero de muy alto impacto.

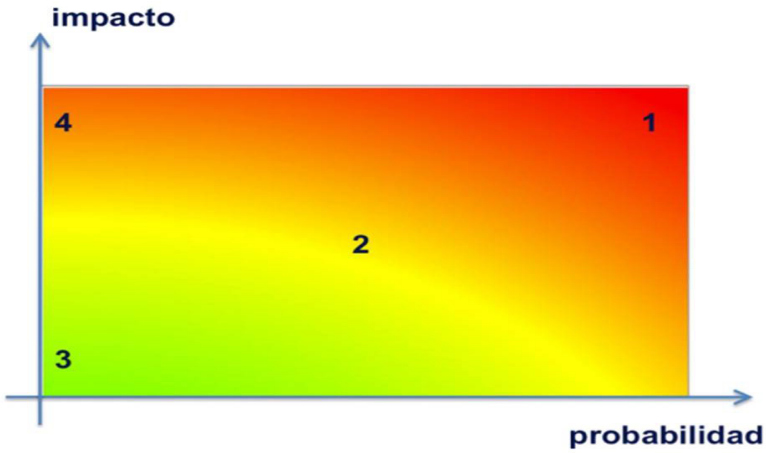

Figura 1. Zonas de riesgo en función del impacto y la probabilidad (Ministerio de Hacienda y Administraciones Públicas, 2012, 30)

El Ministerio de Hacienda y Administraciones Públicas (2012, 32-34), recomienda implementar contra-medidas adecuadas que minimicen el riesgo, las cuales impactan en el riesgo de dos maneras: reduciendo la probabilidad de un suceso o limitando el daño. Estas contra-medidas o salvaguardas se presentan en diferentes tipos de protección: - De efecto preventivo, son las que reducen la probabilidad de un suceso, las cuales son preventivas, disuasorias y eliminatorias. - que acotan la degradación, siendo minimizadoras, correctivas y recuperativas, y - que consolidan el efecto de los demás, siendo de monitorización, detección, concienciación y administración. Asimismo, recomienda utilizar una

escala de madurez que utilice el factor de corrección de la contra-medida de esta manera al haber modificado el impacto y el riesgo, se genera un impacto residual y un riesgo residual.

Para definir un plan de seguridad informática se requiere un análisis que haya permitido conocer las vulnerabilidades de la organización en materia de seguridad informática. Sobre estas vulnerabilidades se deben realizar propuestas de políticas, procedimientos y medidas que lleven a garantizar la integridad, disponibilidad y confidencialidad de la información. Si un plan de seguridad informática está bien encaminado se convertirá en un proceso transversal que apoya a la organización tanto en los procesos operacionales como estratégicos al garantizar la protección del activo vital de las organizaciones KPO, es decir, la protección de los datos e información, ya que la información como núcleo del negocio puede ser utilizada en cualquier momento, ya sea en la operación y préstamo de servicios o también para la toma de decisiones del negocio. Por esta razón es que un plan de seguridad informática enfocado en la protección de la información tendrá un alcance total en la organización, en sus procesos y en su personal.

Por su factor diferenciador (manejo de activos intangibles relacionados con propiedad intelectual y *know-how*, que se convierten en activos críticos a considerar para entender que el activo que se está protegiendo ya no es información sino conocimiento), en el sector KPO se deben considerar elementos y estrategias para el plan de seguridad informática:

- Un respaldo legal[9] debido al activo crítico que se maneja en organizaciones que cuentan con un área de seguridad informática o contratan un servicio con terceros,
- Personal para implementar técnicas de *hacking* destinadas a verificar nuevas vulnerabilidades en los sistemas y tener un control preventivo y correctivo continuo,
- El compromiso de la dirección de la organización con los planes de seguridad informática. Este punto es muy importante y se hace énfasis en la segunda etapa del modelo propuesto en el referente conceptual, no todos los ataques de *hacking* se realizan sobre dispositivos tecnológicos, existe el campo de la ingeniería social que explota la vulnerabilidad del personal a través de la manipulación para obtener información, es un campo con técnicas muy difíciles de definir que no permiten anticiparse, es por esto que se recomienda

9 Por ejemplo, acuerdos de confidencialidad o acuerdos de consentimiento entre las partes para manipular información en entornos controlados o cualquier otro documento o contrato propio de la empresa.

brindar capacitación al personal para que no sean objeto de manipulación o engaño.
- La realización de pruebas de penetración en los sistemas para identificar vulnerabilidades y corregirlas, realizar pruebas a nivel de ingeniería social en un entorno controlado, para comprobar si en el personal existe algún eslabón débil por el cual se pueda acceder a información privilegiada, este tipo de pruebas y verificaciones permiten que la seguridad informática se presente en un entorno sostenible. Uno de los mecanismos de defensa más efectivos en contra de las amenazas, de acuerdo con Kilinc & Cagal (2016), es establecer sistemas de alerta temprana, sistemas inteligentes de detección de amenazas para entender el comportamiento, la capacidad y la intención del adversario.

Se debe entender que los modelos de sistemas de gestión de seguridad de la información están generalmente pensados para que se implementen de manera continua, es decir, con un funcionamiento cíclico de sus etapas, por esto es importante el compromiso de la empresa con la seguridad informática para darle la importancia que realmente debe tener en la organización.

3. Conclusiones

Debido a que en el contexto colombiano la tercerización de servicios del conocimiento es un tema reciente y en general no se encuentran estudios directamente relacionados a los Sistemas de Gestión de Seguridad de la Información en empresas KPO, este documento es un primera aproximación a este tema al plantear sugerencias que se adecuen al entorno de las empresas KPO, sirviendo como un referente para guiar la implementación de mecanismos que busquen mantener la disponibilidad, integridad y confiabilidad de los activos informáticos.

Como señalan Soomoro, Shah & Ahmed (2016, 215). la tecnología ha incrementado de manera ilimitada las oportunidades de negocio, pero por otro lado ha generado nuevos retos, que incluyen cambios dramáticos en el diseño de las organizaciones, en los sistemas de administración de datos e información, implicaciones tecnológicas y riesgos, lo cual señala que la seguridad informática debe tener un papel más fundamental en las empresas y evolucionar acorde con estas, convirtiendo la seguridad informática en un proceso transversal y con un enfoque holístico.

En los modelos de SGSI se pueden encontrar falencias al estar enfocados solamente en procesos y no en personas, cuando uno de los principales retos de la seguridad informática es prevenir los ataques de ingeniería social. La tecnología sirve como herramienta para procesar, almacenar, distribuir, organizar y manipular información, pero son las personas las que realmente lo interpretan como algo valioso, el factor humano es el eslabón más débil en la cadena de seguridad, afirma Pacheco (2013, 668). Lo que demuestra que la seguridad informática no debe tener un enfoque puramente técnico, además se debe considerar un administrativo donde también se definan políticas de seguridad para las personas.

La tercerización de servicios es una tendencia que se dado en el ámbito mundial y que está incursionando en el colombiano, muestra la influencia de evolución tecnológica en las empresas en su competitividad, y generando nuevos retos que las empresas deben considerar, por ejemplo la protección de datos e información, tanto para las empresas KPO como para cualquier empresa que implemente tecnologías en sus procesos.

Como trabajo futuro se espera contribuir con un análisis más profundo de diferentes empresas KPO en la industria colombiana, la propuesta de un modelo más detallado basado en nuevos hallazgos para la implementación de SGSI en el sector KPO con un enfoque hacia las personas y una metodología para evaluar estos modelos en las empresas KPO. Actualmente hay una limitante ya que no se encuentran trabajos que se enfoquen principalmente en la seguridad informática de las empresas KPO, demostrando la poca importancia que se le ha dado a la protección de datos e información, específicamente en empresas de este tipo donde los datos e información son el insumo principal.

Referencias bibliográficas

ALARCÓN VILLAMIL, Nelson Orlando; GÓMEZ CAICEDO, Melva Inés & STELLIAN, Rémi (2016). Perfil competitivo de empresas de tercerización de procesos de Bogotá: análisis de componentes principales [en línea]. En: AD-minister, No. 29 (jul-dic). p. 101-120 · e-ISSN 2256-4322 <http://publicaciones.eafit.edu.co/index.php/administer/article/view/3491/3180> [consulta: 28/11/2017]

ARDON BARAHONA, Lesly Susana & ESCOBAR REYES, Rebeca Esmeralda (2016). La eficacia de los derechos laborales de los trabajadores contratados por empresas *outsourcer* en El Salvador [en línea]. Trabajo de grado (Licenciada en Ciencias Jurídicas). San Salvador (El Salvador): Universidad de El Salvador, Facultad de Jurisprudencia y Ciencias Sociales, Escuela de Ciencias Jurídicas. 165 p + Anexos <http://ri.ues.edu.sv/12770/1/LA%20EFICACIA%20DE%20LOS%20DERECHOS%20LABORALES%20DE%20LOS%20TRABAJADORES%20CO.pdf> [consulta: 01/12/2017]

BENCHIMOL, Daniel (coord.) (2011). Hacking desde Cero: conozca sus vulnerabilidades y proteja su información [en línea]. Buenos Aires (Argentina): Fox Andina - Gradi. 192 p. ISBN: 978-987-1773-03-9 <http://www.tugurium.com/docs/HakingCero.pdf> [consulta: 17/01/2016]

CASTRO ESCOBAR, Edisson Stiven & SERNA GÓMEZ, Héctor Mauricio (2016). Calidad del Empleo en Organizaciones de Servicios de Contact-Center en Manizales, Colombia [en línea]. En: Revista Latinoamericana de Ciencias Sociales, Niñez y Juventud, Vol. 14, No. 1 (ene-jun). Manizales (Colombia): Centro Internacional de Educación y Desarrollo Humano (Cinde) - Universidad de Manizales. p. 205-219. ISSN: 1692-715X <http://dx.doi.org/10.11600/1692715x.14113140814>, <http://www.scielo.org.co/pdf/rlcs/v14n1/v14n1a14.pdf> [consulta: 28/11/2017]

CURIE, Wendy L; MICHELL, Vaughan & ABANISHE, Oluwakemi (2008). Knowledge Process Outsourcing in financial services: The vendor perspective [online]. In: European Management Journal, Vol. 26, No. 2, (dic). Amsterdam (Netherlands): Elsevier B.V. p. 94-104. ISSN: 0263-2373. <http://www.sciencedirect.com/science/article/pii/S0263237307001211> [consult: 17/01/2016]

FAZLIDA, Mohd Razali & SAID, Jamaliah (2015). Information Security: Risk, Governance and Implementation Setback [online]. In: Procedia Economics and Finance, Vol. 28 Amsterdam (Netherlands): Elsevier B.V. p. 243-248. ISSN: 2212-5671 <http://www.sciencedirect.com/science/article/pii/S2212567115011065>, <https://doi.org/10.1016/S2212-5671(15)01106-5> [consult: 11/03/2016]

GARCÍA, Luis Hernando (2017). Caracterización de los actores del "clúster" BPO – ITO – KPO en Cali (2014 – 2016) [en línea]. En: Documentos de trabajo FCEA, No. 30. Santiago de Cali (Colombia): Pontificia Universidad Javeriana. p. 4-34. e-ISSN: 2422-4642 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064206> [consulta:06/12/2017]

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN, ICONTEC (2013). NTC-ISO-IEC 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Bogotá (Colombia): Icontec. 25 p.

JIDIGA, Goverdhan Reddy & SAMMULAL, Porika (2013). The Need of Awareness in Cyber Security with a Case Study [online]. In: 4th International Conference on Computing Communications and Networking Technologies, ICCCNT, (4-6/07/2013), Tiruchingode (India): IEEE. e-ISBN: 978-1-4799-3926-8. <http://ieeexplore.ieee.org/document/6726789/>, <https://doi.org/10.1109/ICCCNT.2013.6726789> [consult: 01/07/2016]

KILINC, Hakan & CAGAL, Ugur (2016). A reputation based trust center model for cyber security [online]. In: 4º International Symposium on Digital Forensics and Security, ISDFS 2016 (25-27/04/2016). Little Rock (AR, USA): IEEE. p. 1-6. ISBN: 978-1-4673-9865-7. <https://doi.org/10.1109/ISDFS.2016.7473508>, <http://ieeexplore.ieee.org/document/7473508/> [consult: 12/07/2016]

LAUMER, Sven; BLINN, Nadine & ECKHARDT, Andres (2012). Opening the Black Box of Outsourcing Knowledge Intensive Business Process – A longitudinal Case Study of Outsourcing Recruiting Activities [online]. In: 45th Hawaii International Conference on Systems Science, HICSS 2012 (4-7/01/2012), Maui (HI, USA): IEEE. Proceedings of the HICSS 2012, p. 3827-3836. ISSN: 1530-1605. <https://doi.org/10.1109/HICSS.2012.459>, <http://ieeexplore.ieee.org/document/6149262/> [consult: 19/12/2015]

LONGFEI, Liu; ZHONGLI, Gao; YING, Li & LIJUN, Liang (2013). Risk Management of the Intellectual Property in Knowledge Process Outsourcing [online]. In: 6th International Conference on Information Management, Innovation Management and Industrial Engineering, ICIII 2013 (23-24/11/2014). Xi'an (China): IEEE. Proceedings of the ICIII 2013. Piscataway (NJ, USA): The Institute of Electrical and Electronics Engineers, IEEE. p. 147-150. ISBN: 978-1-4799-0245-3. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6703536> [consulta: 07/03/2016]

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS (2012). MAGERIT - versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [en línea]. Madrid (España): Ministerio de Hacienda y Administraciones Públicas. Libro I – Método. 127 p. <https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html> [consulta: 08/05/2016]

MOYO, Moses; ABDULLAH Hanifa & NIENABER, Rita C. (2013). Information Security Risk Managementin Small-Scale Organisations: A Case Study of Secondary Schools Computerised Information Systems [online]. In: Information Security for South Africa, 2013 (14-16/08/2013), Johannesburg (South Africa): IEEE. p. 1-6. e-ISBN: 978-1-4799-0808-0 <http://ieeexplore.ieee.org/document/6641062/>, <https://doi.org/10.1109/ISSA.2013.6641062> [consult: 04/08/2016]

NANCYLIA, Merry; MUDJTABAR, Eddy K; SUTIKNO, Sarwono & ROSMANSYAH, Yusep (2014). The Measurement Design of Information Security Management System [online]. In: 8th International Conference on Telecommunication Systems Services and Applications, TSSA 2014, (23-24/10/2014), Kuta (Indonesia): IEEE. e-ISBN: 978-1-4799-7447-4 <http://ieeexplore.ieee.org/document/7065914/>, <https://doi.org/10.1109/TSSA.2014.7065914> [consult: 26/08/2016]

PACHECO, Federico G. (2013). The need for Formal Education on Information Security [online]. In: IEEE Latin America Transactions, Vol. 11, No. 1 (Feb). Campinas (Brazil): IEEE Region 9. p. 668-670. ISSN: 1548-0992 <https://doi.org/10.1109/TLA.2013.6502882>, <http://ieeexplore.ieee.org/document/6502882/> [consult:03/09/2016]

PÁEZ GONZÁLEZ, Daniel David (2017). Propuesta de metodología de evaluación de seguridad informática, aplicada a proveedores de servicios de pequeñas y medianas empresas (pyme), que accedan a información de personas físicas en el municipio de Toluca, estado de México [en línea]. Trabajo terminal de grado (Maestro en Alta Dirección en sistemas de Información). Toluca (México): Universidad Autónoma del Estado de México, Facultad de Contaduría y Administración. 118 p. <https://ri.uaemex.mx/bitstream/handle/20.500.11799/67693/TTG_Daniel_Paez.pdf?sequence=1&isAllowed=y> [consulta: 26/11/2017]

PROGRAMA DE TRANSFORMACIÓN PRODUCTIVA (2014). Caracterización y formulación estratégica regional del sector BPO, KPO e ITO en Colombia [en línea]. Bogotá (Colombia): Ministerio de Comercio, Industria y Turismo, Programa de Transformación Productiva. 302 p. <http://www.andi.com.co/camarabpo/Documents/Estudios%20y%20Estadisticas/Caracterizaci%C3%B3n%20y%20Estrategia%20Regional_2013.pdf> [consulta: 29/11/2017]

RAMALINGAM, S; ARCHANA BAI, S & VIMALA, K (2007). Knowledge Process Outsourcing - A new revolution [online]. In: IET-UK International Conference, Information and Communication Technology in Electrical Sciences, ICTES 2007 (20-22/12/2007), Tamil Nadu (India): IET. p. 1069-1073. ISBN: 9780863419379. <http://ieeexplore.ieee.org/document/4735952> [consult: 02/02/2016]

SOOMORO, Zahoor Ahmed; SHAH, Mahmood Hussain & AHMED, Javed (2016). Information Security management needs more holistic approach: A literature review [online]. In: International Journal of Information Management, Vol. 36, No. 2 (Apr). Amsterdam (The Netherlands): Elsevier. p. 215-225. ISSN:0268-4012 <https://doi.org/10.1016/j.ijinfomgt.2015.11.009>, <http://www.sciencedirect.com/science/article/pii/S0268401215001103> [consult: 07/09/2016]