UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE RIESGOS INFORMÁTICOS EN EL SISTEMA CONTABLE SYSCOFIN DE LA EMPRESA GOLDENSHRIMP S.A DE LA CIUDAD DE MACHALA

PINEDA ENCARNACION KARLA MARICELA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE RIESGOS INFORMÁTICOS EN EL SISTEMA CONTABLE SYSCOFIN DE LA EMPRESA GOLDENSHRIMP S.A DE LA CIUDAD DE MACHALA

PINEDA ENCARNACION KARLA MARICELA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

ANÁLISIS DE RIESGOS INFORMÁTICOS EN EL SISTEMA CONTABLE SYSCOFIN DE LA EMPRESA GOLDENSHRIMP S.A DE LA CIUDAD DE MACHALA

PINEDA ENCARNACION KARLA MARICELA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

ORDÓÑEZ BRICEÑO KARLA FERNANDA

MACHALA, 04 DE FEBRERO DE 2019

MACHALA
04 de febrero de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado Análisis de riesgos informáticos en el sistema contable SYSCOFIN de la Empresa Goldenshrimp S.A de la Ciudad de Machala, hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

ORDÓÑEZ BRICEÑO KARLA FERNANDA
0705031003
TUTOR - ESPECIALISTA 1

GONZALEZ SANCHEZ JORGE LUIS
0703333898
ESPECIALISTA 2

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 3

Fecha de impresión: lunes 04 de febrero de 2019 - 15:38

Urkund Analysis Result

Analysed Document:	PINEDA ENCARNACION KARLA MARICELA_PT-011018.pdf (D47135692)
Submitted:	1/23/2019 4:04:00 AM
Submitted By:	titulacion_sv1@utmachala.edu.ec
Significance:	3 %

Sources included in the report:

URKUND actualizacion tecnologica medidas seguridad centro computo ronald cuenca.docx (D40698090)
Idrovo CAPTULO 2 - PARTE 2.docx (D12717871)

Instances where selected sources appear:

2

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, PINEDA ENCARNACION KARLA MARICELA, en calidad de autora del siguiente trabajo escrito titulado Análisis de riesgos informáticos en el sistema contable SYSCOFIN de la Empresa Goldenshrimp S.A de la Ciudad de Machala, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 04 de febrero de 2019

PINEDA ENCARNACION KARLA MARICELA
0704651611

RESUMEN

El crecimiento económico ha ido a la par del desarrollo tecnológico, por lo que se ha convertido en parte fundamental para las empresas, con el fin de aumentar la eficiencia de sus actividades comerciales y financieras. En la actualidad no se concibe que una empresa carezca de recursos informáticos, siendo necesario que los empresarios o emprendedores tomen conciencia de la trascendencia de los sistemas informáticos para agilizar las actividades organizacionales, así como contar con un mayor control sobre éstas. Las empresas para ejercer un control de sus actividades laborales cuentan con sistemas contables que hoy en día son de índole informático, agilizando las actividades contables y financieras de una empresa. Sin embargo, al ser un bien informático posee ciertos riesgos que pudieran vulnerar su seguridad en perjuicio de la información confidencial que pudiera tener la organización. Esta situación ha dado lugar a la presente investigación para analizar los riesgos en la plataforma informática SYSCOFIN de la empresa Goldenshrimp S.A. de la ciudad de Machala. Haciendo uso de la metodología descriptiva, técnicas de investigación bibliográfica y de las directrices mencionadas por la norma COSO, para establecer la matriz de riesgos del sistema contable.

Palabras claves: Seguridad, información, fraudes informáticos, riesgos, sistemas contables.

ABSTRACT

Economic growth has gone hand in hand with technological development, which is why it has become a fundamental part for companies, in order to increase the efficiency of their commercial and financial activities. At present it is not conceivable that a company lacks computer resources, being necessary for entrepreneurs or entrepreneurs to become aware of the importance of computer systems to streamline organizational activities, as well as having greater control over them. Companies to exercise control of their work activities have accounting systems that are now computer-based, streamlining the accounting and financial activities of a company. However, being a computer asset, it has certain risks that could damage its security to the detriment of confidential information that the organization may have. This situation has led to the present investigation to analyze the risks in the SYSCOFIN computer platform of the company Goldenshrimp S.A. from the city of Machala. Making use of the descriptive methodology, bibliographic research techniques and the guidelines mentioned by the COSO standard, to establish the risk matrix of the accounting system.

Keywords: Security, information, computer fraud, risks, accounting systems.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

INTRODUCCIÓN

El desarrollo tecnológico se ha convertido en un aliado para el progreso comercial. La informática empresarial consiste en el uso de tecnologías para incrementar la gestión organizacional, siendo un recurso fundamental para el control de las actividades comerciales dentro de la empresa.

Hoy en día no se concibe que una empresa carezca de recursos informáticos, siendo necesario que los empresarios o emprendedores tomen conciencia de la trascendencia de los sistemas informáticos para agilizar las actividades organizacionales, así como contar con un mayor control sobre éstas.

Parte importante de una organización son los sistemas contables que hoy en día son de índole informático, agilizando las actividades contables y financieras de una empresa. Sin embargo, al ser un bien informático posee ciertos riesgos que pudieran vulnerar su seguridad en perjuicio de la información confidencial que pudiera tener la organización. Como lo señala (Corda, Viñas, & Coria, 2017) el riesgo informático imposibilita cumplir con los objetivos organizacionales por su afectación al funcionamiento de un sistema tecnológico. Esta situación ha dado lugar a la presente investigación con el fin de identificar los riesgos en la plataforma informática SYSCOFIN de la empresa Goldenshrimp S.A. de la ciudad de Machala. Para ello se utilizó la metodología descriptiva con la finalidad de establecer el nivel de riesgo del sistema contable. Para Abreu (2014) el método descriptivo permite realizar una exposición narrativa, numérica sobre el objeto de estudio. Como técnica se hizo uso de la bibliografía y de las directrices mencionadas por la norma COSO, que según Alarcón y Torres (2017) sirven para establecer la matriz de riesgos del sistema contable.

1. FUNDAMENTACIÓN TEÓRICA

1.1. Seguridad de la información

La información permite obtener conocimientos de una determinada situación de interés para la persona, esta se expone de forma diaria por los acontecimientos locales y mundiales donde las tecnologías de información y comunicación se han convertido en las protagonistas, creyéndose que en pocos años las personas estarán intercomunicadas permanentemente a través de redes de telefonía móvil que se han convertido en los equipos con menos brecha digital (Ramírez, 2013). Para García y Vidal (2016) la cantidad de computadoras presentes en empresas y organizaciones ha sido significativo en los últimos tiempos, situación que ha aumentado los riesgos informáticos. Donde las personas y empresas deben de tomar medidas precautelares para poner a buen resguardo su información contenida en estos medios.

Para Miranda, Valdés, Pérez, Portelles y Sánchez (2016) los ataques informáticos se originan por la fragilidad o baja confiabilidad del software, malware, equipos celulares, personas de la empresa, piratas informáticos conocidos como hackers, situación que da lugar a un 69% de inconvenientes con la seguridad informática en perjuicio de la persona naturales o jurídica que ve violentada su privacidad.

Los virus informáticos han evolucionado a una velocidad alta, esto producto del uso masivo del internet, siendo una de las finalidades del virus, aparte de dañar la información, obtener datos clasificados y de acceso privado como claves de seguridad, números de tarjetas de crédito (Quiroz, 2017).

Por tal situación existen normas como las ISO 17799:2005 (Organización Internacional de Normalización) señalan que la información se ha convertido en un activo de gran valor, debiendo las organizaciones implantan seguridades informáticas para su protección (Alexander, 2012).

Los activos de información pueden ser clasificados de la manera siguiente:

- Documentos contractuales.
- Posicionamiento de la empresa.

- Softwares presentes en aplicaciones informáticas, sistema operativo, plataformas digitales.
- Equipos de comunicación
- Documentos informativos como el manual de usuario.
- Talento humano de la empresa.
- Clientes y usuarios de la organización
- Recursos tecnológicos tales como computadoras, laptops, redes, accesorios.

Caiza y Bolaños (2014) indican la necesidad de que las organizaciones evalúen los riesgos debiendo aplicar políticas para salvaguardar los datos ante cualquier tipo de acción o actividad que pueda ser considerada como una amenaza.

1.2. Sistema de gestión de seguridad de la información

Desde correos electrónicos internos hasta materiales de ventas y estados financieros, las organizaciones de todos los tamaños de todas las industrias manejan grandes cantidades de información cada día. Para una organización, esta información es una ventaja competitiva. El objetivo de un Sistema de gestión de seguridad de la información (SGSI) es proteger la información (Mesquida, Mas, Amengual, & Cabestrero, 2010).

Un sistema de gestión de seguridad de la información (SGSI) es un conjunto de políticas y procedimientos para la gestión sistemática de los datos confidenciales de una organización. El objetivo de un SGSI es minimizar el riesgo y asegurar la continuidad del negocio al limitar de manera proactiva el impacto de una violación de la seguridad.

Un SGSI generalmente aborda el comportamiento y los procesos de los empleados, así como los datos y la tecnología. Puede dirigirse a un tipo particular de datos, como los datos de los clientes, o puede implementarse de una manera integral que se convierta en parte de la cultura de la empresa.

Para Yánez y Yánez (2012) la ISO 27001 es una especificación para crear un SGSI. No exige acciones específicas, pero incluye sugerencias de documentación, auditorías internas, mejoras continuas y acciones correctivas y preventivas.

1.3. Fraudes informáticos

Con el desarrollo de la tecnología, también ha evolucionado los fraudes informáticos, donde un pirata informático puede sustraer recursos económicos e información sin dejar rastros en perjuicio de la organización (Arcentales & Caycedo, 2017). Situación que dio lugar a la toma de medidas de seguridad para salvaguardar los recursos valiosos que posee toda empresa.

1.4. Vulnerabilidades y amenazas

Vulnerabilidad es una debilidad que tiene un recurso informático que puede ser explotada por una amenaza poniendo en riesgo la información (Quiroz, 2017).

1.5. Riesgos en los sistemas contables

Díaz, Pérez y Proenza (2014) exponen que las organizaciones de todo tipo y tamaño deben de contar con políticas para salvaguardar la información ante cualquier tipo de riesgo o amenaza, a esto se suma que se debe de contar con los respectivos respaldos que den lugar a la continuidad al restablecer y recuperar la información en caso que ésta haya sido vulnerada.

Donde la gestión de riesgo a través de un sistema de control interno sirve a la empresa para tomar acciones eficaces frente a alguna contingencia o vulnerabilidad que afecten al normal desarrollo de la empresa (López, Albanese, & Sánchez, 2014). Siendo conveniente que las organizaciones implanten los SGSI (sistema de gestión de seguridad de la información) para precautelar la información clasificada y confidencial que manejan diariamente las empresas en base a sus operaciones. De esta forma el SGSI respalda la información ante cualquier pérdida:

- Privacidad de la información con acceso de las personas autorizadas por la empresa o jefes departamentales.
- Resguardo de la información de forma integral.
- Disponibilidad del sistema de manera permanente para el acceso oportuno del usuario.

1.5.1. Controles preventivos

Las empresas deben estar preparadas para reducir cualquier fraude a las que pudieran estar expuestas, implementando y supervisando controles internos preventivos para disuadir cualquier intento de violentar la seguridad informativa de una organización (Salas & Reyes, 2015).

1.5.2. Controles detectivos

Permiten a las empresas activar alertas ante la aparición de alguna desviación avisando al responsable del sistema para que actúe ante algún problema (Estupiñan, 2015). La organización al contar con controles detectivos permite estar permanentemente vigilantes ante cualquier intromisión a los sistemas.

1.5.3. Controles correctivos

Los controles correctivos sirven para mejorar aquellas desviaciones que se encontraron en los controles detectivos (Estupiñan, 2015). Por esta situación los sistemas suelen actualizarse de manera periódica para prevenir cualquier tipo de ingreso no autorizado que puedan perjudican a la empresa al robar o borrar la información contenida en los sistemas.

2. DESARROLLO

2.1. Metodología

Para el análisis de riesgo informático del sistema contable se aplicaron las Normas COSO que contiene lineamientos para optimizar los controles dentro de una empresa a través de una gestión eficiente de la seguridad en todos sus niveles (Mantilla, 2015).

Con estas normas se elaboró una matriz de riesgos para conocer las falencias que posee el sistema contable de la empresa, para su posterior optimización y mejora. Los pasos para analizar los riesgos fueron:

- Establecimiento del contexto: Es la información relacionada con la empresa tales como nombre, sector comercial, personas que acceden al sistema, ubicación, servicio, funciones del sistema (Alarcón & Torres, 2017).

- Identificación de riesgos, vulnerabilidades y amenazas: Se observa e identifica a través del sistema las posibles, eventualidades que pueden causar un daño a la información confidencial (Alarcón & Torres, 2017).
- Evaluación de riesgo: Sirve para plasmar en una matriz la probabilidad de ocurrencia e impacto de los riesgos (Alarcón & Torres, 2017).
- Sugerencias de controles preventivos, detectivos y correctivos: Se sugieren aplicar controles preventivos, detección, correctivos, disminuyendo la probabilidad de ocurrencia de impacto de los riesgos (Alarcón & Torres, 2017).

Con esta información se procede a elaborar la matriz de riesgos que sirve a la empresa para tomar medidas preventivas para incrementar la seguridad de su sistema contable.

2.2. Resultados

1. Establecimiento del contexto

Tabla 1: Contexto del sistema contable

Información de la empresa	**Goldenshrimp S.A.**
Sector comercial	Se dedica a la producción y comercialización de camarón para la exportación.
Personas que acceden al sistema	Contador Auxiliar contable 1 Auxiliar contable 2
Ubicación del sistema	Departamento de contabilidad
Servicios ofrecidos por el software	Sistema contable que cumple con las normativas contables y legales vigentes para dar cumplimiento a las actividades financieras y tributarias de la empresa.
Funciones del software	· Facturación · Retenciones · Guías de remisión · Notas de crédito · Envío de la factura por email a clientes. · Reportes financieros · Ingreso y egreso de mercadería · Cierre de inventario · Control de la cuenta caja · Control y administración de las cuentas por pagar y cobrar · Registro de las compras y ventas diarias · Conciliación bancaria · Generación de código de barras · Anexos transaccionales · Balance general · Estado de resultados · Flujo de caja

Fuente: Investigación directa
Elaboración: La autora

2. Identificación de vulnerabilidades, amenazas y riesgos

Tabla 2: Identificación de vulnerabilidades, amenazas y riesgos

Vulnerabilidades	Amenazas	Riesgos
Mala elaboración de contraseñas	Ingreso al sistema contable con facilidad	Pérdida de información por la inexistencia de claves seguras
Inadvertencia en el software contable	Acceso a la base de datos del sistema	Pérdidas económicas por no emitir alertas al acceso del sistema
Desviación de la información	Integridad del sistema	Pérdida de credibilidad por la falta de reportes de IP

Fuente: Investigación directa
Elaboración: La autora

3. Evaluación de riesgos

Tabla 3: Matriz de riesgos

Nº	Factor de riesgo	Probabilidad			Impacto			Causas del factor de riesgo	Recomendaciones	Responsable
		Alto	Medio	Bajo	Alto	Medio	Bajo			
1	Inexistencia de claves seguras		X		X			La gerencia no analizó este requerimiento como política de seguridad	Exigir a usuarios del sistema contable ingresar claves de tipo alta	Gerente y contador
2	Falta de alertas o notificaciones no autorizadas			X	X			El personal que desarrolló el software no incorporó esa característica dentro del mismo.	Solicitar a la compañía del software agregar las alertas o notificaciones no autorizadas.	Compañía de software
3	Faltante de reportes sobre usuario IP cuando se ingresa, modifica o elimina un registro contable			X	X			La compañía que desarrolló el software no tomó en cuenta dicha cualidad.	Solicitar a la compañía del software agregar las alertas o notificaciones para cada uno de los ingresos al sistema ya sea para ingresar, modificar o eliminar algún registro contable.	Compañía de software

Elaboración: La autora

Se pudo detectar que el sistema contable SYSCOFIN posee pocos riesgos destacando su confiabilidad y además es amigable, cuenta con manual de procedimientos, goza de una interfaz agradable. Sin embargo, se ven amenazadas por vulnerabilidades exponiendo la información confidencial de la empresa Goldenshrimp S.A. Los riesgos encontrados son:

Inexistencia de claves seguras. El sistema sí cuenta con perfil de usuario, pero las claves ingresadas son de nivel bajo. La probabilidad de ocurrencia es media pero su impacto es alto. El riesgo podría darse al momento de enviar los equipos a mantenimiento donde persona ajena a la empresa puede tener acceso a los archivos dentro de las carpetas generadas por el sistema contable. La gerencia y el jefe del área contable debe exigir a los usuarios cambiar de claves por unas más seguras.

Falta de alertas en notificaciones: Las alertas sobre acceso no autorizado tienen una probabilidad baja pero el impacto sería alto. Esto se debe a que el personal de la empresa que tiene acceso al sistema solamente son el contador y los dos auxiliares contables. Sin embargo, se deben de tomar las medidas precautelares para evitar cualquier intromisión de personas ajenas a la empresa.

Faltantes de reporte sobre usuario IP: La probabilidad de ocurrencia es baja pero el impacto es alto. El acceso al sistema solo lo hace el personal autorizado. Se debería solicitar a la empresa diseñadora del sistema contable su actualización para que la empresa cuente con reportes de las personas que ingresan al sistema.

El factor de riesgo ocasiona que exista la posibilidad de pérdida de información dentro de la empresa o a su vez se paralicen las operaciones organizacionales por la falta de identidad del sistema por ende se estableció la probabilidad de ocurrencia sea baja con un impacto alto.

4. Dar sugerencias de controles preventivos, detectivos, correctivos para disminuir la probabilidad de ocurrencia de impacto de los riesgos

La empresa Goldenshrimp S.A. de la ciudad de Machala debe tomar medidas preventivas y correctivas para aminorar la probabilidad de ocurrencia por la pérdida o modificación de la información contable y financiera de la empresa que está a cargo del sistema contable.

La gerencia y el contador deberían de exigir al personal contable el ingreso de contraseñas de tipo alta, esto es ingresar letras minúsculas y mayúsculas, números, y teclas alternativas (*, /, +, –) dentro de las políticas de seguridad de la información, y como norma general de la empresa.

Se debe solicitar a la compañía desarrolladora del software contable SYSCOFIN que el sistema pueda emitir alertas o notificaciones cuando el personal no autorizado está manipulando el sistema para poder ingresar a la información contable.

También se debe solicitar al equipo que diseño el software reportes sobre el usuario, hora el IP que han ingresado al sistema ya sea para, modificar o eliminar registros contables, para llevar un control más exhaustivo de la información contable de la empresa.

3. CONCLUSIONES

Los sistemas contables son herramientas informáticas de amplio uso en las empresas ecuatorianas, procediéndose a realizar un análisis del riesgo informático en el sistema SYSCOFIN que posee la empresa Goldenshrimp S.A. localizada en Machala. Se aplicó las normas COSO para realizar un análisis de riesgo informático en que se determinó tres amenazas relacionadas a la seguridad del sistema SYSCOFIN como son el acceso al sistema, alertas sobre acceso no autorizado y su integridad.

Se identificaron tres riesgos: 1) inexistencia de claves seguras, 2) falta de alerta en notificaciones, 3) faltante de reportes sobre usuario IP. Las probabilidades son medias y bajas pero el impacto en cada una de ellas es alto. Exponiéndose recomendaciones que van desde ingresar claves de alta seguridad, solicitar a la compañía diseñadora del software agregar alertas o notificaciones por ingresos no autorizados, además de solicitar reportes de los ingresos de los usuarios para tener un mayor control del sistema contable.

Los riesgos expuestos pueden perjudicar a la empresa a través del robo, daño, eliminación de la información ocasionando pérdidas económicas a la empresa que podrían paralizar las actividades económicas y comerciales en perjuicio de sus integrantes.

BIBLIOGRAFÍA

Abreu, J. L. (Diciembre de 2014). El método de la investigación. *Daena: International Journal of Good Conscience, 9*(3), 195-204.

Alarcón, F., & Torres, M. d. (2017). Evaluación de control interno y gestión del riesgo aplicando el informe Coso I, II, III; en los procesos administrativos y financieros de las entidades públicas. *Revista Publicando, 4*(11), 32-48.

Alexander, A. (2012). *Análisis y evaluación del riesgo de información: Un caso de la banca. Aplicación del ISO 27001:2005.* Lima: Pontificia Universidad Católica del Perú.

Arcentales, D., & Caycedo, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las Ciencias, 3*(1), 157-173.

Caiza, M., & Bolaños, F. (2014). Las implementaciones de las normas de seguridad de la información: estudio de caso la Sociedad de Lucha Contra el Cáncer del Ecuador. *Revista electrónica de Computación, Informática, Biomédica y Electrónica*(3), 2-22.

Corda, M. C., Viñas, M., & Coria, M. K. (2017). Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. *Palabra Clave, 7*(1), 1-18.

Díaz, Y., Pérez, Y., & Proenza, D. (2014). Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín. *Ciencias Holguín, 20*(2), 1-14.

Estupiñan, R. (2015). *Administración de riesgos E.R.M. y la auditoría interna.* Madrid: Ecoe Ediciones.

García, G., & Vidal, M. J. (2016). La informática y la seguridad. Un tema de importancia para el directivo. *INFODIR*(22), 47-58.

López, M. d., Albanese, D. E., & Sánchez, M. (2014). Gestión de riesgos para la adopción de la computación en nube en entidades financieras de la República Argentina. *Contaduría y Administración, 59*(3), 61-88.

Mantilla, S. A. (2015). *Estándares/Normas Internacionales de Aseguramiento de la Información Financiera (ISA/NIA): Los fundamentos, los estándares y las implicaciones.* Madrid: Ecoe Ediciones.

Mesquida, A., Mas, A., Amengual, E., & Cabestrero, I. (2010). Sistema de gestión integrado según norma ISO 9001, ISO/IEC 2000 e ISO/IEC 27001. *1856-8327, 6*(3), 25-34.

Miranda, M., Valdés, O., Pérez, I., Portelles, R., & Sánchez, R. (2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. *Revista Cubana de Ciencias Informáticas, 10*(2), 14-26.

Quiroz, S. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias, 3*(5), 676-688.

Ramírez, J. L. (2013). Humanización del aprendizaje en la era de la información: una arista andragógica. *Revista Electrónica "Actualidades Investigativas en Educación, 13*(3), 1-18.

Salas, J., & Reyes, N. (2015). Modelo propuesto para la detección de fraudes por parte de los auditores internos basado en las Normas Internacionales de Auditoría. *Cuaderno Contable, 16*(42), 579-623.

Yánez, J., & Yánez, R. (2012). Auditorías, mejora contínua y normas ISO: Factores claves para la evolución de las organizaciones. *Ingeniería Industrial. Actualidad y Nuevas Tendencias, 3*(9), 83-92.