MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

GUÍA PRÁCTICA PARA REALIZAR AUDITORÍA A LA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN CON ENFOQUE EN EL CONTROL INTERNO EN LAS INSTITUCIONES DEL ESTADO ECUATORIANO.

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información.

Por el estudiante:
Lenín Isrrael NARVAEZ TARANTO.

Bajo la dirección de:
Cesar Martín GONZALES ARBAIZA.

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Agosto de 2018

Guía práctica para realizar auditorías a la gestión de tecnologías de la información, con enfoque en el control interno en las instituciones del estado ecuatoriano.

Practical guide to perform audits to the management of information technologies, with a focus on internal control in the institutions of the Ecuadorian state.

Lenín Israel NARVÁEZ TARANTO[1]
Cesar Martín GONZALES ARBAIZA[2]

Resumen

El presente artículo propone una guía práctica para realizar auditorías a la gestión TI, que permita al profesional de auditoría incorporar una metodología para llevar con éxito el ejercicio de evaluación a los componentes de un sistema de gestión de diferentes ámbitos, esto basado en las mejores prácticas y la legislación ecuatoriana vigente. En la investigación se recogió las normas ecuatorianas de auditoria gubernamental emitidas por la contraloría general del estado como organismos de control en el estado ecuatoriano, así como también las normas de control interno y el marco internacional para la auditoria de los sistemas de gestión – ISO 19011:2011, se realizó un análisis y un cotejo de las normas determinando las coincidencias y los puntos importantes. Posteriormente, con el desarrollo de la investigación se propone una guía, cuyas etapas describen los pasos elementales para realizar una auditoría, desde la etapa de compresión organizacional hasta el seguimiento de la implementación de las recomendaciones. Hacemos notar que con una adecuada planeación, nos brinda los lineamientos y directrices claros para la ejecución y comunicación de los hallazgos identificados en el ejercicio de auditoria, cuyo resultado en el informe final redunda en la mejora continua a la gestión de TI.

Palabras clave: | Auditoría, Tecnologías de la Información, Sistemas de Gestión.

Abstract

This article proposes a practical guide to perform IT management audits, which allows the audit professional to incorporate a methodology to successfully carry out the evaluation exercise to the components of a management system in different areas, based on best practices and current Ecuadorian legislation. The research included the Ecuadorian government audit standards issued by the state comptroller general as control bodies in the Ecuadorian state, as well as internal control standards and the international framework for auditing management systems - ISO 19011 : 2011, an analysis and a comparison of the rules was made, determining the coincidences and the important points. Subsequently, with the development of the research a guide is proposed, whose stages describe the elementary steps to perform an audit, from the organizational compression stage to the follow-up of the implementation of the recommendations. We note that with adequate planning, it provides us with clear guidelines and guidelines for the execution and communication of the findings identified in the audit exercise, the result of which in the final report results in the continuous improvement of IT management.

Key words | Audit, Information Technologies, Management Systems

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo– Ecuador. E-mail lnarvaez@uees.edu.ec.
[2] Ingeniero de Sistemas, Post Grado en Redes y Telecomunicaciones, Master en Administración de Negocios, Examinador de Fraude Certificado. E-mail cgonzales@uees.edu.ec

INTRODUCCIÓN

En los albores del siglo del XXI se enfatizaba a la tecnología moderna como un eje dinamizador mundial y transformador en los procesos de almacenamiento y distribución de la información en las empresas, donde las TIC globalizaron las relaciones organizacionales marcando momentos de intercambios sin distinción de fronteras nacionales. (Sørnes, Sætre, Stephens, & Browning, 2004). Hoy en día, introducir en las organizaciones un sistema basado en tecnologías de la información provoca efectos importantes en los procesos internos, comportamiento de los colaboradores y lo resultados de la gestión de TI (Cuel & Ferrario, 2009).

En la actualidad, la información y los avances de la tecnología como recursos claves y los beneficios que brindan, permiten a las organizaciones iniciar operaciones de inversión en tecnología de información, con enfoques de retorno de la inversión, sin embargo, en muchos casos no se evalúa el costo beneficio, riesgos e impacto que estas puedan tener causando pérdidas significativas en las instituciones (Emigdio, 2011).

Por otro lado, según la encuesta de Deloitte (2016) sobre tendencias de seguridad de la información y ciber riesgos en Latinoamérica se centra en que cuatro de cada diez organizaciones han sufrido brechas de seguridad en los últimos dos años, mientras que menos del 20% de las organizaciones cuentan con centros de operaciones de seguridad, esto indica que las empresas están expuestas a riesgos debido a su fuerte vinculación con la tecnología digital, y en este contexto las debilidades básicas de seguridad siguen apareciendo en los procesos de auditorías de TI.

Existen otros desafíos vinculados al gobierno, riesgos y auditorias de tecnologías de la información, para Security Advisor (2017) las personas en las empresas son la parte más vulnerable y critica en los sistemas de gestión, el humanware[3] es un componente importante, complejo y muchas veces olvidado, la tecnología no se gestiona por si sola involucra principalmente un elemento psicológico por parte del ser humano para alcanzar las metas de seguridad que se requiere en las organizaciones.

Por otra parte, según Vieites (2015) existe un importante incremento de los problemas legales por la indebida utilización de los recursos de TI, a causa de la falta de normas claras y desconocimiento del marco regulatorio local, por todo aquello, es importante considerar el talento humano como el eje principal en los aspectos de seguridad de la información, fomentando la sensibilización y compromiso de los altos funcionarios para la aprobación de normas, políticas y procedimientos sobre el uso adecuado de los recursos de TI dentro y fuera de la organización.

Los esfuerzos del gobierno del Ecuador por incorporar un modelo que integre los cuatro actores importantes en una sociedad organizada – Gobierno, Ciudadanos, Sector Productivo y Servidores Públicos – llevaron a incorporar un plan de Gobierno electrónico, que según la ONU[4] (2016) se refiere al uso adecuado de las TIC para mejorar los servicios e información brindados a los ciudadanos, así como también mejorar la gestión pública e incrementar la transparencia. Por esto, el gobierno del Ecuador promueve el uso del software libre mediante decreto ejecutivo con el objetivo de alcanzar soberanía y autonomía tecnológica (SNAP, 2008)[5], la aplicación de un esquema gubernamental de seguridad de la información basado en la norma internacional ISO 27001 mediante el acuerdo ministerial No. 166 cuyo objetivo es implementar un marco de buenas prácticas de seguridad que deben aplicar las instituciones públicas que

[3] Personal involucrado en la operación, programación, uso y explotación de los recursos de TI.

[4] Organización de las Naciones Unidas.

[5] Secretaria Nacional de la Administración Pública.

dependan de la función ejecutiva (DINARDAP, 2017)[6].

La inserción en el COIP[7] sobre los delitos electrónicos forma parte del avance jurídico en el Ecuador desde que entró en vigencia, en las que se tipifican los delitos informáticos a la revelación ilegal de base de datos, interceptación de datos, ataques a la integridad de sistemas informáticos, entre otras, no obstante, con referencia al principio de libertad probatoria de los elementos digitales, se requiere de formación profesional en peritaje informático y de los profesionales de derecho en informática jurídica (Páez, 2015).

Se aprecia que en el Ecuador hay una tendencia creciente de uso de las tecnologías de la información y comunicaciones; por lo mismo se requiere de un impulso adecuado para el fortalecimiento, desarrollo y control de las TIC en pro de generar avances en la economía del país.

A pesar de los esfuerzos del gobierno ecuatoriano en el desarrollo del marco regulatorio en materia de seguridades de TI; el desconocimiento de Leyes, normas, acuerdos por parte de los profesionales en auditorias está presente, la falta habilidades en la aplicación de estándares y buenas prácticas de gestión auditorías, hacen que los resultados del ejercicio de evaluación a los sistemas de gestión de seguridad de la información no sean precisos y eficientes, en consecuencia no aporten a la mejora continua del proceso auditado y a la organización.

Según López (2017), el CIO no se empodera de sus roles lo cual no aporta a la consecución de los objetivos de la empresa sobre asuntos tan importantes como la obsolescencia tecnológica, ciberseguridad, gestión de la seguridad de la información y continuidad del negocio, no es capaz de identificar puntos débiles e influir en el CEO para que incorporen un gobierno empresarial en temas cruciales como son las TI y lograr que la tecnología genere un valor estratégico en la empresa.

Kress (2016) refiere que indudablemente el impacto de la transformación de TI está reinventando la función y los procesos de auditoría, esta situación pone en cuestionamiento a las prácticas de auditorías pasadas, por esto requiere alinear la función de auditoria de TI para estos tiempos en base a la legislación y normas internacionales.

De acuerdo al giro del negocio las operaciones que las empresas realizan son complejas y se requiere de habilidades directivas para el cumplimiento de objetivos que deben ser supervisados por un órgano de control que vigile y audite los procesos, la actividad de control cada vez adquiere más relevancia, la auditoria interna objetiva agrega valor y mejora las operaciones, permite la consecución de los objetivos mejorando la eficacia en sus procesos permitiendo a los ejecutivos tomar decisiones correctivas para mejorar la administración, beneficio y cumplimiento (Sanchis, 2015).

Aunque los recursos de auditoría de TI son limitados, las organizaciones están comenzando a reconocer la necesidad de tener auditores de TI certificados y dedicados en el personal, ya que los datos muestran esta tendencia al alza con un promedio de personal de auditoría de TI del 18%. Los riesgos tecnológicos deben ser considerados en el proceso de evaluación del riesgo de la auditoría y tratados en el plan de auditoría (Ahia, 2015).

El presente trabajo de investigación tiene como objetivo primordial, presentar una guía práctica para evaluar la gestión de tecnologías de la información, con un enfoque agregador de valor basadas en las Normas de Control Interno, la Norma Ecuatoriana de Auditoría Gubernamental de la Contraloría General del Estado y la Norma

[6] Dirección Nacional de Registro de Datos Públicos.

[7] Código Integral Penal – COIP, vigente desde el 10 de Agosto del 2014

ISO 19011 para la gestión de auditorías a los sistemas de gestión, con el propósito que el auditor pueda combinar estrategias para una efectiva evaluación y valoración a los procesos de TI en las instituciones del estado.

MARCO TEÓRICO

Tecnologías de la Información y Comunicaciones

Para Romani (2009) las TIC[8] son un conjunto innovador de componentes electrónicos (microprocesadores, semiconductores, fibra óptica, etc.) que facilitan el proceso y almacenamiento y transmisión de grandes volúmenes de información con capacidades de distribución por medio de las redes de comunicaciones, en ese contexto, las tecnologías en estos tiempos son importantes y necesaria para transformar y gestionar la información a través de ordenadores, dispositivos móviles y aplicaciones que coadyuvan a crear, modificar, almacenar, proteger, recuperar y distribuir. Las TI motiva la generación e intercambio de conocimiento en favor del fortalecimiento de la sociedad de la información.

Leal (2008) concluye que las TIC en el mundo de hoy es un requisito importante que exige la sociedad con un nivel más alto de dependencia de la misma, quienes logren incorporar una plataforma de TI y desarrollen capacidades intelectuales de uso tendrán mejores capacidades en la toma de decisiones e influirán en la construcción y fortalecimiento de la sociedad del conocimiento.

Auditoria

Los ejercicios de auditorías deben apoyar a la organización, para el Instituto Ecuatoriano de Normalización (2012) auditoria es un "proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría".

Las auditorias son importantes porque alinean a las organizaciones hacia los objetivos estratégicos, los resultados obtenidos deben estrictamente ser observados a fin de que se tome los correctivos necesarios y no generar pérdidas financieras y reputacionales (Flores, 2015).

Contraloría General del Estado

Según la Asamblea Constituyente del Ecuador (2008), la Contraloría General del Estado, es un organismo técnico cuya función principal es controlar la utilización de los recursos del estado así como también dirigir el control administrativo mediante auditorías internas, externas y del control interno a las instituciones que están regidas mediante derecho público y de las entidades privadas que dispongan de recursos públicos, con el objetivo de examinar, comprobar, y evaluar la gestión operativa de entre otras. De los resultados de las evaluaciones y auditorías que la CGE ejerce a las instituciones públicas y privadas que dispongan de recursos públicos[9], se determinan responsabilidades administrativas, civiles e indicios de responsabilidad penal.

Auditoria gubernamental

El propósito de la Auditoria gubernamental es determinar el nivel de cumplimiento de los objetivos y metas organizacionales y proporcionar seguridad a la información generada por la entidad, con el objetivo de motivar toma de decisiones que permitan alcanzar los objetivos trazados. Los preceptos que rigen el desarrollo de una auditoria

[8] Tecnologías de la Información y Comunicaciones

[9] La ley Orgánica de la CGE define a los recursos públicos a todos los bienes, activos, utilidades, acciones, títulos, fondos, participaciones, subvenciones, excedentes y todos los derechos que le pertenecen al estado inclusive prestamos, donaciones u otro título a favor del estado ecuatoriano.

gubernamental son las Normas Ecuatorianas de Auditoria Gubernamental y las Normas Ecuatorianas de Auditoria, dichas normas son de aplicación obligatoria para los auditores del estado y firmas privadas contratadas (General, 2002).

Auditoría de gestión

La auditoría de gestión de acuerdo a la metodología para auditoría de gestión de la Contraloría General del Estado es un examen metódico realizado por un grupo de auditores interdisciplinarios con el fin de evaluar y medir la eficacia de la gestión de una organización en concordancia con los objetivos planteados, en ese mismo sentido, la Ley Orgánica de la Contraloría General del Estado describe a la Auditoria de Gestión como una acción fiscalizadora que evalúa la gestión y el control interno con un talento de humano multidisciplinario para determinar si la ejecución se ha realizado en base a los principios de economía, efectividad y eficiencia (Contraloria General del Estado, 2011).

CLASES DE AUDITORIAS

Auditoría Interna – (AI)

Según la Organización Internacional de Estandarización(2005) la AI, es un mecanismo para identificar riesgos y no conformidades, esta conlleva a realizar el seguimiento de las no conformidades identificadas en procesos de auditorías anteriores, donde se debe evaluar las acciones ejecutadas para el cumplimiento de sus objetivos, en ese sentido los altos ejecutivos deben instaurar un proceso de auditoría interna independiente para evaluar el o los sistemas de gestión implementados en la organización, con el propósito de obtener evidencias que permitan justificar el cumplimiento de los requisitos identificados, pues bien, la auditoria interna se encarga de evaluar la eficiencia y eficacia de una organización. Pues bien, ISO (2016) describe que la forma como se administre el proceso de auditoría interna se convierte en el factor crítico para garantizar la eficacia de un sistema de gestión.

Control Interno

La Ley Orgánica de la Contraloría General del Estado describe que el control interno establece un proceso cuya responsabilidad recae en la máxima autoridad y todo el personal en los diferentes niveles de cada institución cuyo fin es proveer seguridad razonable a los recursos públicos y se logren los objetivos institucionales, por consiguiente el control interno genera las condiciones necesarias para el ejercicio de una auditoria externa a cargo de la Contraloría General del Estado[10] (CGE, 2002).

Auditoría Externa.

Es la evaluación crítica, sistemática de un sistema de información de una unidad de negocio realizado por un profesional sin relación de dependencia o vínculos profesionales con la organización auditada, usa buenas prácticas de auditorías y formula una opinión autónoma sobre los sistemas de gestión auditados y los controles internos aplicados formulando también consejos para el mejoramiento de sus procesos (Jiménez, 2017). La auditoría externa puede ser solicitada por diferentes sectores como clientes y entes reguladores.

Auditoria de Tecnologías de la Información

Según Cynthus (2017), la auditoria de TI son actividades de control para evaluar las Tecnologías de la Información así como también el entorno en la que se desenvuelve la seguridad de la información, tomando como referencia la normativa nacional y buenas prácticas internacionales, los principales beneficios de la

[10] La Contraloría General del Estado establece acciones preventivas como capacitaciones que coadyuven la consecución de la misión y visión de las Instituciones públicas.

auditoria de TI comprende en determinar el nivel de cumplimiento de la normativa, verificar que los servicios de TI son eficientes y mitigar posibles riesgos.

Es un examen objetivo, sistemático y profesional para evaluar la eficiencia, fiabilidad y utilidad de los recursos y servicios de TI, encierra también un análisis integral de la organización en torno al talento humano, segregación de funciones, seguridades y actividades de procesamiento de datos (Fallis, 2013).

Auditoria del Gobierno de TI.

Los altos ejecutivos en una organización tienen grandes responsabilidades que demandan tiempo y mucho cuidado, probablemente sus conocimientos son limitados en aspectos de TI y en otras aristas corporativas, de igual manera los CIO[11] por lo general no forman parte del modelo de gobierno corporativo, la función de TI se vuelve invisible cuando los procesos de TI funcionan con normalidad y al momento de asignar presupuesto surgen cuestionamientos con enfoques de gastos, esto es porque la información crítica que se maneja en las organizaciones es intangible, por lo tanto, la participación y el compromiso de los altos ejecutivos en el diseño y ejecución de las estrategias y políticas empresariales (Gelbstein, 2017).

Auditoria a los Sistemas de Gestión.

La auditoría de los sistemas de gestión es de vital importancia para implementar acciones preventivas y correctivas al detectarse anomalías. Están relacionadas con la supervisión que realizan los directivos y permiten con una adecuada planificación percibir mecanismos de mejora continua en los procesos de la organización (Moncayo, 2016).

Para que las auditorias sean efectivas y sirvan como mecanismos para la gestión de políticas y controles deben soportarse en los principios que la norma ISO 19011[12] recomienda, tales como, integridad, presentación honesta, cuidado profesional, confidencialidad, independencia y enfoque basado en la evidencia (ISOTOOLS, 2016).

Hallazgos de auditoría

De acuerdo a la Guía metodológica para la auditoría de gestión (Contraloria General del Estado, 2011) un hallazgo de auditoría se concibe a toda información que según el criterio profesional del auditor, identifica los hechos o circunstancias importantes que impactan significativamente, en el sistema de gestión auditado, estos deben ser descritos en el informe en base a la condición, criterio, causa y efecto.

Por otra parte, según ISO 9001 (2005), un hallazgo es el resultado de evaluar la evidencia obtenida frente a los criterios de auditoria definidos, este puede determinar una fortaleza o debilidad y puede indicar una observación o no conformidad.

Los hallazgos levantados y las conclusiones de una auditoría deben reflejar un nivel de detalle de las actividades ejecutadas en la auditoría, deben estar basados en la evidencia de auditoría suficiente y apropiada. En ese sentido, los hallazgos elaborados por el auditor deben estar debidamente sustentados con documentos de trabajo que respalde el criterio (ISACA, 2013).

Conformidad y No conformidad

No conformidad es el incumplimiento de un requisito obligatorio de las leyes, reglamentos, norma, requisitos del cliente. Frente a una conformidad las organizaciones deben

[11] Chief Information Officer – CIO, Responsable del desarrollo, implementación y operación de la política de TI en la organización, en el contexto ecuatoriano es la persona que tiene el cargo de director de TI.

[12] Estándar reconocido internacionalmente, proporciona directrices para la gestión de un programa de auditoria sobre la planificación y ejecución de una auditoria de un sistema de gestión.

reaccionar evaluando las causas que provocó el hallazgo definiendo e implementando planes de acción que deben ser medidos en su eficacia después de implementar los controles (ISO9001, 2016).

Observación

La observación es la comprobación de hechos o circunstancias significativos obtenidas durante el proceso de auditoría y justificada por evidencias objetivas (Contraloria General del Estado, 2011).

Auditoria de Sistemas de Gestión de Riesgos

Para Kahn (2013) la evaluación del riesgo es un proceso donde se identifican las vulnerabilidades y amenazas, cada una de ellas se debe ponderar la probabilidad y el impacto que estas causarían. Es un ejercicio complejo por cuanto es una actividad repetitiva, progresiva y continua.

De igual manera, Gelbstein (2017) menciona que las auditorias basada en riesgos tiene un enfoque más efectivo con aquellos colaboradores que identifican y evalúan los riesgos en las organizaciones, a través de un taller comunicativo con el área de riesgos, custodios de la información, unidad de tecnologías de la información, concientizando a la alta gerencia, fortaleciendo la función de la auditoria interna, esto indica que mitigar los riesgos emergentes y la responsabilidad de aquello permanece en el grupo auditado.

Auditoria de Sistemas de Gestión de Seguridad de la información

Las auditorias de seguridad de la información son un mecanismo de gestión que las organizaciones emplean para evaluar la eficacia de su sistema basado en buenas prácticas establecidas de la norma ISO 27001 con el propósito de establecer mejoras en cada componente del SGSI, permite gestionar adecuadamente los riesgos y oportunidades para la protección de los activos de información de la organización (Formación, 2017).

De igual forma las organizaciones deben planificar con frecuencia auditorías internas para validar los requisitos establecidos por la norma implementada en temas de seguridad de la información , por lo tanto, también es necesario contar con profesionales con habilidades desarrolladas en el ámbito de auditoria, gestión y seguridad de la información. Así mismo, en la etapa de planificación de la auditoria se debe tener en cuenta los procesos y áreas que tienen que ser auditadas, también se debe contar con los resultados de auditorías anteriores, donde es necesario establecer el alcance, frecuencia y los métodos a utilizarse (ISOTOOLS, 2015).

Según la Universidad Tecnológica Nacional UTN (2017) las auditorias de seguridad de la información se deben efectuar una vez al año bajo la supervisión del Jefe de auditoria de seguridad de la información que debe ser nombrado por la máxima autoridad, los criterios a tener en cuenta en una auditoria deben ser la gestión de activos de información y gestión de información personal de conformidad con las normas locales de protección de datos.

Auditoria de Sistema de Gestión de Continuidad del Negocio.

El proceso de Continuidad del Negocio abarca tópicos como la Planeación para Recuperación de Desastres (DRP), como la Planeación para el Restablecimiento del Negocio. La Recuperación de Desastres es la capacidad para responder a una interrupción de los servicios mediante la implementación de un plan para restablecer las funciones críticas de la organización (Jimenez, 2015).

METODOLOGIA

La investigación tiene un enfoque de tipo cualitativo debido a que recoge información de sobre la norma ISO/IEC 27001:2013 y las normas del estado ecuatoriano en el ámbito de control interno y desarrollo de auditorías. En este proceso se realizaron entrevistas con

profesionales que prestan sus servicios en el área de tecnologías de la información de diferentes instituciones públicas, cuyo objeto es conocer la percepción del ejercicio de auditoría por parte de auditores frente a los criterios agregadores de valor y mejora continua en los procesos de gestión.

Existen estándares, metodologías, modelos a nivel global que fueron desarrolladas metodológicamente con las buenas prácticas, esta fuente de información son oportunidades para la complementariedad en la aplicación de criterios de evaluación, al identificar el o los modelos de referencia a utilizarse, es recomendable utilizar un enfoque top-down, es decir, de arriba hacia abajo empezando desde las definiciones y requerimientos hasta los detalles, de esta forma se obtienen mejores resultados (Olaya, 2018).

GUIA DE AUDITORÍA A LA GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN ENFOQUE DE CONTROL INTERNO.

Para el sector público ecuatoriano, las Normas de Control Interno son guías generales presentadas por el organismos de control como es la Contraloría General del Estado, cuyo objeto es promover una adecuada administración de los recursos públicos y la determinación del correcto funcionamiento en la gestión administrativa de las entidades y organismos del sector público, a fin de buscar la efectividad, eficiencia y economía en la gestión institucional.

Las Normas de Control Interno, se constituyen mediante procedimientos dirigidos a proporcionar una seguridad razonable, para que las entidades evaluadas puedan lograr los objetivos específicos planteados.

Por otro lado, el alcance del presente trabajo de investigación, está delimitado al proceso de TI y la gestión de seguridad de la información basada en las normas de control interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos, normas del grupo 410 de Tecnologías de la Información.

De acuerdo a las normas ecuatorianas de auditoria gubernamental – NEAG, la ISO 19011:2011, norma desarrollada por la Organización Internacional de Normalización (ISO), que establece las directrices para la auditoría de los sistemas de gestión de la calidad, la ISO 27001:2013 como estándar para la gestión de seguridad de la información y las normas de control interno de la contraloría general del estado, son los ejes principales para el desarrollo de la propuesta como guía de auditoría de a la gestión de seguridad de la información en las instituciones del estado ecuatoriano.

Por otra parte, hay que citar que a través del acuerdo ministerial No. 166 emitido el 25 de septiembre del 2013, el estado ecuatoriano dispone la implementación y el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información, a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva. En ese mismo contexto, el Ministerio de Telecomunicaciones, ente rector del Esquema Gubernamental de Seguridad de la Información – EGSI del acuerdo 166, vela por el cumplimiento y seguimiento de la adopción del EGSI.

La Norma ISO 19011, en su cláusula cinco para la auditoría de sistemas de gestión describe el programa de auditoría en su etapa de planeación, el cual está integrado de las siguientes actividades:

1. Establecer los objetivos del programa de auditoría.
2. Determinar y evaluar las oportunidades y riesgos del programa de auditoría.
3. Establecer el programa de auditoría.
4. Implementar el programa de auditoría.
5. Monitorear el programa de auditoría.

6. Revisión y mejora del programa de auditoría.

Las actividades elementales que se deben considerar para la realización de la auditoría son:

1. Iniciar la auditoría.
2. Preparar las actividades de auditoria.
3. Conducir las actividades de auditoría.
4. Preparar y distribuir el reporte de auditoría.
5. Finalizar la auditoría.
6. Auditoría de seguimiento.

La figura 1 muestra el flujo del proceso de la cláusula cinco y seis, que de acuerdo a la norma ISO 19011:2018 se deben considerar para realizar el ejercicio de auditoría a un sistema de gestión, basado en el ciclo de mejora continua PHVA.

	PLANEAR	HACER	VERIFICAR	ACTUAR
PROGRAMA DE AUDITORIA	1. Establecer los objetivos del programa de auditoría.			
	2. Determinar y evaluar las oportunidades y riesgos del programa de auditoría			
	3. Establecer el programa de auditoría	4. Implementar el programa de auditoría	5. Monitorear el programa de auditoría.	6. Revisión y mejora del programa de auditoría
REALIZACIÓN DE LA AUDITORIA	1. Iniciar la auditoría			
	2. Preparar las actividades de auditoria	3. Conducir las actividades de auditoría		
		4. Preparar y distribuir el reporte de auditoría	5. Finalizar la auditoría.	6. Auditoría de seguimiento
	PLANEAR	HACER	VERIFICAR	ACTUAR

Figura 1: Proceso de la cláusula cinco y seis de la norma ISO 19011

Las Normas Ecuatorianas de Auditoria Gubernamental – NEAG, rigen al sector público y están basadas en las Normas de Auditoria Generalmente Aceptadas – NAGA, estas normas son de aplicación y cumplimiento obligatorio por los auditores.

Las Normas Ecuatorianas se estructuran de la siguiente forma:

1. Relacionadas con el auditor gubernamental.
2. Relacionadas con la planificación de la auditoria gubernamental.
3. Relativas con la ejecución de la auditoria gubernamental.
4. Normas relativas al Informe de la auditoria gubernamental.

Relacionadas con el auditor gubernamental.

La Contraloría General del Estado y las autoridades del evaluado, exigirá el cumplimiento de los requisitos establecidos para el auditor en los siguientes aspectos:

a. Título profesional que le acredite los conocimientos específicos para ejercer la función.
b. Experiencia profesional según el nivel de responsabilidad y las funciones a realizar.
c. No tener impedimentos legales para desempeñar cargos públicos.

El auditor gubernamental deberá acreditar capacidades técnicas que garanticen su productividad y eficiencia. Mantendrá independencia, una conducta imparcial y objetiva durante el ejercicio de la auditoria de conformidad a las disposiciones legales y el código de ética profesional y además mantendrá absoluta reserva en el desempeño de sus actividades como auditor gubernamental.

Planificación de la auditoría gubernamental,

Se planificarán las actividades anuales considerando la aplicación de criterios relacionados al riesgo y oportunidad. El contenido de los planes deben estar alineados con los objetivos y políticas institucionales; estos exámenes deben concentrar estrategias para medir la eficacia, la eficiencia y la efectividad de la gestión en el uso de recursos públicos y el logro de resultados en función de los objetivos trazados.

La planificación de la auditoría asegura una adecuada atención en temas y problemas de absoluta importancia. En la elaboración del plan se tendrá en cuenta lo siguiente:

a. Conocimiento de la entidad.
b. Comprensión de los sistemas de información administrativa, financiera y de control interno.
c. Riesgo e importancia relativa.
d. Naturaleza, importancia y alcance de los procedimientos.
e. Coordinación, dirección, supervisión y revisión.

Según el plan de auditoria trazado, se debe designar formalmente al equipo de auditoria que se encargaran de realizar el examen correspondiente, cuya designación deberá contar con un jefe de equipo, para esto se debe velar por el cumplimiento de los requisitos relacionados con el auditor gubernamental.

Ejecución de la auditoría gubernamental.

En la ejecución de la auditoría gubernamental se evaluará el cumplimiento de las leyes y reglamentos aplicables al desarrollo de las actividades de gestión y de apoyo de los entes públicos.

El auditor gubernamental revisará el marco regulatorio de la organización a la cual se está realizando el examen, debido a que los organizaciones públicas se rigen generalmente por leyes, ordenanzas, decretos y están sujetas a disposiciones legales y reglamentarias específicas.

El auditor deberá llevar un registro ordenado detallado y completo de las actividades realizadas y conclusiones obtenidas. La evidencia reunida por el auditor en el desarrollo de su tarea, son el vínculo entre el trabajo de planeamiento, de ejecución y del informe de auditoría.

El auditor obtendrá evidencia suficiente mediante la aplicación de técnicas de auditoria y deben tener las siguientes características:

a. Suficiente.- Proporciona seguridad razonable con un riesgo mínimo.
b. Competente.- La evidencia debe ser válida y confiable.
c. Pertinente.- Relación entre la evidencia y su uso.

El propósito también de las NEAG, está encaminada a determinar si existen sucesos importantes que afecten a la entidad auditada.

INFORME DE AUDITORÍA GUBERNAMENTAL.

Aquí se mostrarán los casos significativos identificados como el incumplimiento de leyes y reglamentos, en la medida de lo posible incluir, el pronunciamiento de los funcionarios responsables del ente, programa o actividad objeto de la auditoría, relacionados a los resultados comunicados y a las medidas correctivas aplicadas por la administración durante el proceso de la auditoría. Los comentarios, conclusiones y recomendaciones se deben presentar en orden de importancia y con criterio objetivo.

En base a las normas ISO 19011 y las Normas Ecuatorianas de Auditoría Gubernamental, en la

siguiente tabla se muestra las etapas de la guía para realizar una auditoría al sistema de gestión de tecnologías de la información.

No	ETAPAS DE LA GUÍA	ACTIVIDADES	PRODUCTOS/ENTREGABLES
1	Comprensión de la organización	1.- Levantamiento de información sobre el estado actual, características, infraestructura, procesos de negocios y sistemas de información que los soportan.	Organigrama de la institución. Ficha técnica de los sistemas de información. Diagrama de los procesos de negocios.
2	Definir el alcance y objetivos de la auditoría	1. Análisis de situación de la organización o proceso a evaluar. 2. Análisis de entorno. 3. Determinación de los objetivos y alcance de la auditoría.	Necesidades y requerimientos de las partes interesadas.
3	Elaborar el plan de auditoría	1. Designar el equipo auditor. 2. Estimación del tiempo y recursos. 3. Definir criterios de auditoria.	Orden de trabajo. Plan de auditoría.
4	Estudio y evaluación del control interno	1. Identificar los controles existentes en los procesos de negocio y sistemas de información. 2. Evaluar el nivel de protección de los controles existentes.	Informe de la eficiencia de los controles aplicados y su brecha de seguridad.
5	Evaluación del cumplimiento de las disposiciones legales y reglamentarias	1. Evaluar el cumplimiento de Normativa vigente	Grado de cumplimiento de la normativa.
6	Obtención de evidencias	1. Recabar pruebas de auditorías suficientes, pertinentes y competentes.	Banco de pruebas
7	Evaluación de los resultados obtenidos	1. Análisis de las observaciones de auditoría y puntos de mejoras para los controles. 2. Identificar las causas / efecto de las observaciones para la organización. 3. Conclusiones preliminares de auditoría del ejercicio de auditoría.	Conclusiones de los resultados.
8	Comunicación de hallazgos de auditoria	1. Convocar a involucrados a la comunicación de hallazgos de auditorias	Informes y actas de comunicación y entendimiento de hallazgos. Informe de descargos.
9	Informe preliminar de auditoria	1. Resumen de Hallazgos. 2. Analizar informes de descargos. 3. Elaborar conclusiones generales y específicas de la auditoría con criterio objetivo, imparcial y constructivo en orden de importancia. 4. Estructurar informe de acuerdo a las NEAG	Resumen de hallazgos. Informe de auditoría.
10	Convocatoria a la conferencia final	1. Convocar a la conferencia final a la máxima autoridad, delegados, equipo de auditoria e involucrados que no pertenezcan a la organización.	Acta de conferencia final firmada por los convocados
11	Presentación del informe final de auditoria	1. Organizar expediente y archivo con hojas de trabajo.	Informe final de auditoria y expediente con los soportes
12	Implementación y seguimiento de las recomendaciones	1. Elaboración de planes de acción. 2. Establecer fechas de cumplimiento. 3. Emitir informes de seguimiento.	Planes de acción y remediación. Cronograma de cumplimiento. Informes.

A continuación se describe a detalle tópicos que son importantes en el desarrollo de la auditoría.

Verificación de la información.

La información relevante que se obtenga durante el ejercicio de auditoria debe ser recolectada y verificada mediante procesos adecuados, de otra forma no debe ser considerada como evidencia de auditoria.

La figura 2 muestra una clara visión del tratamiento que debe realizarse a la información recolectada en las actividades de auditoría.

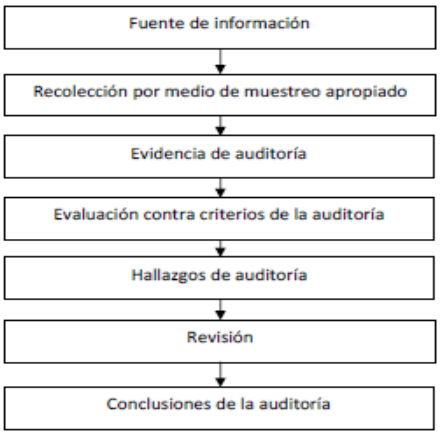

Figura 2 Visión general del proceso de recolección y verificación de la información. Fuente: Norma Internacional ISO 19011.

Revisión de documentos

La documentación de gran importantica debe ser revisado con el objeto de reunir la información necesaria para preparar las actividades de auditoría, debe incluir los documentos y registros del sistema de gestión auditado, así como los informes de auditorías anteriores.

HALLAZGO	PLANES DE ACCIÓN
No conformidad mayor	Acción correctiva inmediata
No conformidad menor	Acción preventiva
Observación	Acción de mejora

Figura 3 - Planes de acción para los tipos de hallazgo.

Generación de hallazgos de auditoría.

La evidencia obtenida en el ejercicio debe ser comparada y evaluada con los criterios de auditorías seleccionados en la planificación cuyo propósito es determinar los hallazgos de auditoria. Los hallazgos pueden derivar en una conformidad, no conformidad.

Las no conformidades deben ser expuestas en donde debe existir un reconocimiento y aceptación por parte del auditado a fin de reconocer que las evidencias son coherentes y que el hallazgo categorizado como no conformidad son entendidos por todos los involucrados.

Para efectuar un levantamiento de los hallazgos por proceso o por cada buena práctica de gestión se elaboran las características de un hallazgo, en consideración de: condición, criterio, causa y efecto; La condición debe ser expresada en base al sistema de gestión evaluado relacionado con la evidencia de auditoría (Encalada, 2016).

Para determinar los hallazgos de auditoría se debe tener en cuenta lo siguiente:

a) Control y seguimiento de conclusiones de auditorías anteriores.
b) Requisitos del cliente.
c) Oportunidades de mejora.
d) Dimensión de la muestra.
e) Categorización de los hallazgos de auditoría.

Para el registro de las conformidades se debe observar lo siguiente:

a) Determinar los criterios de auditoria.
b) Evidencia de la auditoría.
c) Declaración de la conformidad.

Para el registro de las no conformidades se debe observar lo siguiente:

a) Descripción de los criterios de auditoría.
b) Declaración de la no conformidad.
c) Evidencia de auditoría.

Conclusiones de auditoría

De acuerdo a la metodología para auditoría de gestión de Contraloria General del Estado

(2011), el juicio del auditor para establecer las conclusiones deberá observar los resultados de la evaluación relacionados al logro de las metas, en ese mismo sentido, para preparar las conclusiones de auditoría el equipo auditor debe reunirse para revisar y verificar que los hallazgos estén conformes a los criterios de auditoria establecidos y los objetivos planteados en el plan, según la norma internacional ISO 19011(2011) los aspectos que se deben considerar para generar las conclusiones de auditoría son: el grado de conformidad en relación a la efectividad del sistema de gestión auditado en el cumplimiento de los objetivos, la implementación y mejora continua del sistema de gestión.

Reunión de cierre

El líder de auditoria como facilitador debe ejecutar la reunión de cierre en donde previamente se debe convocar a los altos ejecutivos y los líderes de los procesos para presentar los hallazgos encontrados y las conclusiones de auditoria del sistema de gestión auditado.

Cuando los hallazgos levantados reflejan una no conformidad mayor que pueda impactar severamente a los procesos de la organización y su continuidad, se debe definir de forma inmediata los planes de acción correctivas para mitigar las debilidades identificadas. De otra forma, cuando los hallazgos categorizados como no conformidad menor u observación se debe establecer y acordar con el auditado los tiempos para la elaboración de los planes de acción preventivos y su cumplimiento en función del intervalo de tiempo establecido para tratar los hallazgos de auditoría.

Durante la reunión de cierre se debe cubrir los siguientes aspectos:

- Prevenir a la audiencia que las evidencias obtenidas está basada en una muestra de información disponible.
- La estructura del reporte de los hallazgos.
- Tratamiento de los hallazgos y las posibles consecuencias de no hacerlo.
- Dar lectura a los hallazgos encontrados y las conclusiones de auditoría.

Las discrepancias suscitadas en la reunión entre el auditor y el auditado se debe tratar y resolverse de otra forma, al no encontrar solución entre las partes se deberían registrar las opiniones vertidas.

Si la organización ha regulado en sus procedimientos de auditoria y tratamiento de hallazgos o en su defecto en los acuerdos contractuales u objetivos de auditoría se han considerado que en los resultados de los ejercicios de auditoria se establezcan oportunidades de mejora de encontrarse, para lo cual, se debe hacer énfasis que dichas recomendaciones no son obligatorias.

CONCLUSIONES

Como resultado del presente trabajo de investigación refleja que llevar a cabo una adecuada planificación de la auditoría a cualquier sistema de gestión como fase inicial en las instituciones públicas, permite comprender el contexto de la empresa y sus procesos, define el objetivo y el alcance de auditoría, marca las directrices para lograr identificar los recursos, los procedimientos y los principales problemas que puedan presentarse en la organización en la fase de ejecución. Logra centrar los esfuerzos del equipo auditor en las áreas de mayor riesgo, por lo que se convierte en una estrategia agregadora de valor para obtener resultados que sirvan como soporte a la gestión y generen continuidad en la empresa.

Aplicando la presente guía, el auditor designado para realizar un ejercicio de auditoría al proceso de tecnologías de la información, podrá evaluar los controles existentes en una institución pública soportando su criterio de auditoria en la norma de control interno para las entidades, organismos

del sector público y de las personas jurídicas que dispongan de recursos públicos, normas expedidas por la Contraloría General del Estado cuyo cumplimiento es obligatorio para todas las instituciones regidas por el estado ecuatoriano.

Garantizar la absoluta independencia del equipo auditor tanto en actitud y apariencia en los procesos y actividades asignadas a ser auditadas permitirá evitar los conflictos de intereses. De la misma forma, para los ejercicios de auditorías internas, los auditores deben ser independientes de las funciones laborales en la organización de tal manera que los hallazgos y conclusiones de auditoria estén soportados en elementos convictorios detectados en los procesos de evaluación.

Se evidenció la existencia de normas, estándares, acuerdos y reglamentos expedidos por el órgano de control pertinente, que regulan al marco de trabajo del proceso de tecnologías de la información en las instituciones públicas del Ecuador, sin embargo, no existe una metodología específica para llevar a cabo una auditoría de tecnologías de la información en un contexto público donde se incorporen las prácticas elementales de evaluación a un sistema de gestión.

Esta propuesta permitirá contribuir como semilla para trabajos futuros, sobre la planificación de auditoría interna basada en riesgos, soportada en las Normas Internacionales para la Práctica Profesional de Auditoría, tomando como referencia a la norma ISO 19011 versión 2018, la misma que establece un marco de análisis con un enfoque a la gestión de riesgos en todo el ciclo de vida del ejercicio de auditoria.

REFERENCIAS BIBLIOGRÁFICAS

Ahia. (2015). IT Audit & Information Security Survey. Retrieved from https://www.ahia.org/assets/Uploads/pdfUpload/WhitePapers/AHIAITAuditAndInformationSecuritySurvey.pdf

Asamblea Constituyente del Ecuador. (2008). Constitución del Ecuador. *Registro Oficial*, 80. Retrieved from https://www.corteconstitucional.gob.ec/images/contenidos/quienes-somos/Constitucion_politica.pdf

CGE. (2002). Base legal y normativa. Retrieved from http://www.contraloria.gob.ec/Normatividad/BaseLegal

Contraloria General del Estado. Guía metodológica para auditoría de gestión (2011).

Contraloria General del Estado. Guía metodológica para auditoría de gestión (2011). Ecuador.

Cuel, R., & Ferrario, R. (2009). The Impact of Technology in Organizational Communication. *Nursing and Clinical Informatics: Socio-Technical Approaches*.

Cynthus. (2017). ¿CONOCES QUÉ ES LA AUDITORIA DE TECNOLOGÍAS DE INFORMACIÓN? Retrieved from https://www.cynthus.com.mx/blog/auditoria-y-consultoria/auditoria-en-ti/

Deloitte. (2016). La evolución de la Gestión de Cyber Riesgos y Seguridad de la Información. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Deloitte 2016 Cyber Risk Information Security Study - Latinoamérica - Resultados Generales vf (Perú).pdf

Dirección Nacional de Registro de Datos Públicos. (2017). UNA NORMA QUE GARANTIZA LA SEGURIDAD DE LA INFORMACIÓN. Retrieved from http://www.datospublicos.gob.ec/2017/01/06/una-norma-que-garantiza-la-seguridad-de-la-informacion/

Emigdio, A. (2011). MAIGTI : Metodología para la Auditoría Integral de la Gestión de la Tecnología de Información. *ÉTICA Y GESTIÓN*, (October 2008).

Encalada, C. (2016). *Guía de auditoría para la evaluación del control interno de seguridad de la información con enfoque COBIT 5: caso Universidad Católica de Cuenca (UCACUE).*

Fallis, A. . (2013). Guia de auditoria de TI. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Flores, S. (2015). Auditoría de sistemas de

información: objetivo y razones para implementarla. Retrieved from https://www.gestiopolis.com/auditoria-de-sistemas-de-informacion-objetivo-y-razones-para-implementarla/

Formación, B. V. (2017). Auditor Interno de Sistemas de Gestión de Seguridad de la Información ISO 27001:2013. Retrieved from http://www.bureauveritasformacion.com/auditor-interno-de-sistemas-de-gestion-de-seguridad-de-la-informacion-ISO-27001-2013-1964.aspx

Gelbstein, E. (2017). Auditoría básica de SI: Preparación para la auditoría de nuevos riesgos, Parte 1. *ISACA Journal*, *1*. Retrieved from https://www.isaca.org/Journal/archives/2017/Volume-1/Pages/preparing-for-auditing-new-risk-part-1-spanish.aspx

General, C. (2002). Normas Ecuatorianas de Auditoria Gubernamental - NEAG. Retrieved from http://www.contraloria.gob.ec/documentos/normatividad/neag-fin.pdf

INEN. (2012). Directrices para la auditoria de los sistemas de gestión. *INEN*, *2011*.

International Organization for Standardization. Norma Internacional ISO 9000 (2005).

ISACA. (2013). *Estándar de auditoría y aseguramiento de SI 1401 Reportes*.

ISACA. (2015). Guía de Auditoría y Aseguramiento de SI 2201 Planificación de la Asignación. Retrieved from https://m.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2201_gui_Spa_0415.pdf

ISACA. (2016). *CISA*.

ISO. (2005). Auditando la eficacia de la auditoría interna. *ISO 9001 Auditing Practices Group Guidance on : Expected Outcomes*, 1–4.

ISO. (2016). ISO 9001 Auditing Practices Group Guidance on : Expected Outcomes. Retrieved from https://committee.iso.org/files/live/sites/tc176sc2/files/documents/ISO 9001 Auditing Practices Group docs/Auditing to ISO 9001 2015/APG-InternalAudit2015.pdf

ISO 19011. (2011). ISO 19011:2011 Directrices para la auditoría de sistemas de gestión. *2011*, *2011*, 59. Retrieved from http://www.uesp.gov.co/uaesp_jo/images/controlInterno/Normatividad SIG/Auditor&#65533;a Interna de Gesti&#65533;n - ISO-19011-2011.pdf

ISOTOOLS. (2015). La auditoría del Sistema de Gestión de Seguridad de la Información. Retrieved from http://www.isotools.pe/auditoria-sistema-de-gestion-de-seguridad-de-la-informacion/

ISOTOOLS. (2016). ISO 19011: Directrices para la Auditoría de los Sistemas de Gestión. Retrieved from https://www.isotools.org/2016/05/16/iso-19011-directrices-auditoria-sistemas-gestion/

ISOTOOLS EXCELLENCE. (2014). ISO 27001: Auditorías internas del SGSI. Retrieved from https://www.pmg-ssi.com/2014/12/iso-27001-auditorias-internas-del-sgsi/

Jimenez, M. (2015). BCP - AUDITORÍA I. Retrieved from https://prezi.com/vprh-u52ze_l/bcp-08-auditoria-i/

Jiménez, Y. (2017). Auditoria externa. Retrieved from https://www.gerencie.com/auditoria-externa.html

Juan José Páez. (2015). Conferencia: “Delitos electrónicos en el Código Orgánico Integral Penal". Retrieved from http://www.colabpi.pro.ec/index.php/noticias/23-el-colegio/noticias/732-conferencia-delitos-electronicos-en-el-codigo-organico-integral-penal

Kahn, R. (2013). Information Security: Risk Assessment & Management. Retrieved from https://www.computer.org/web/no-batteries-required/content?g=7187424&type=blogpost&urlTitle=information-security%3A-risk-assessment-%26-management

Kress, R. (Bob) E. (2016). Transformar la función de auditoría de TI - Seguir el camino digital. *ISACA Journal*, *1*.

Leal, E. T. (2008). Las tecnologías de la información y comunicaciones (TIC) y la brecha digital : su impacto en la sociedad de México. *Revista de Universidad y Sociedad Del Conocimiento*, *4*(2007), 1–8. https://doi.org/http://dx.doi.org/10.7238%2Frusc.v4i2.305

López, J. C. (2017). El CIO debe influir en el Directorio y el CEO, para crear valor en la Tecnología. Retrieved from http://www.itahora.com/analisis-y-tendencias/el-cio-debe-influir-en-el-directorio-y-el-ceo-para-crear-valor-en-la-tecnologia/?lipi=urn%3Ali%3Apage%3Ad_f

lagship3_pulse_read%3BZrVL82KYQgqMVdgO54F5xg%3D%3D
Moncayo, C. (2016). Importancia de la auditoría en los sistemas de gestión. Retrieved from https://www.incp.org.co/importancia-de-la-auditoria-en-los-sistemas-de-gestion/
Olaya, J. (2018). ¿Cuáles son las referencias apropiadas para las mejores prácticas globales de la Gerencia de Proyectos?
Romani, J. C. C. (2009). El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento. *Zer - Revista de Estudios de Comunicación*, *14*, 285–318. https://doi.org/10.4067/S0718-13372003000200001
Sanchis, J. (2015). Importancia de la Auditoría Interna en las Organizaciones. Retrieved from https://auditool.org/blog/auditoria-interna/3289-importancia-de-la-auditoria-interna-en-las-organizaciones
Secretaría Nacional de la Administración Pública. (2008). Software Libre. Retrieved from http://www.administracionpublica.gob.ec/software-libre/
Security Advisor. (2017). La importancia del factor humano en la seguridad de la información. Retrieved from http://www.sadvisor.com/2017/09/04/la-importancia-del-factor-humano-en-la-seguridad-de-la-informacion/?lipi=urn%3Ali%3Apage%3Ad_flagship3_feed%3BRzk%2FS4bsTuSTfpdQ49PTHg%3D%3D
Sørnes, J. O., Sætre, A. S., Stephens, K. K., & Browning, L. D. (2004). The reflexivity between ICTs and business culture: Applying Hofstede's theory to compare Norway and the United States. *Informing Science*, *7*, 1–30.
United Nations Department of Economic and Social Affairs. (2016). *UN E-government survey 2016. E-Government in Support of Sustainable Development*. https://doi.org/10.1016/S1369-7021(02)00629-6
UTN. (2017). Auditor Interno en Gestión de Seguridad de la Información ISO 27001–ISO 19011. Retrieved from http://sceu.frba.utn.edu.ar/course/auditor-interno-norma-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion/
Vieites, A. G. (2015). La Importancia Del Factor Humano En La Se- Guridad Informática, 1–10.