Auditoría Interna de un Sistema Integrado de Gestión de Seguridad de la Información - SGSI basado en la Norma NTC ISO 19011:2012

Maldonado Peña Johann Camilo
Universidad Piloto de Colombia
johann.maldonadosec@gmail.com

Abstract - is presented below the guidelines and steps "guide" to be carried out, an audit of Management Systems Information Security - ISMS, herein audit procedures are established that may apply to commercial organizations, government, service providers, etc. Regardless of the type, size or nature thereof. These steps provide an overview of the activities and tasks that an auditor must perform, at the time of the evaluation and monitoring of the implementation, maintenance and continuous improvement of an ISMS, in order to assess their conformity with ISO / IEC 27001: 2013.

Resumen – A continuación se presentan las directrices y pasos "guía" que se deben llevar a cabo, para la realización de una auditoría de sistemas de gestión de seguridad en la información - SGSI, en el documento se establecen procedimientos de auditoría que pueden ser aplicables a organizaciones comerciales, gubernamentales, proveedores de servicios, etc. Sin importar el tipo, tamaño o naturaleza de las mismas. Estos pasos brindan una visión general de las actividades y tareas que un auditor debe llevar a cabo, al momento de realizar la evaluación y seguimiento a la implementación, mantenimiento y mejora continua de un SGSI, con el fin de evaluar su conformidad con la norma ISO/IEC 27001:2013.

Palabras Clave –Auditado, Auditor, Auditoría, Criterios de auditoría, equipo auditor, Evidencia de la auditoría, hallazgos de la auditoría, Sistema de gestión, SGSI

I. INTRODUCCIÓN

En la actualidad las ciencias computaciones y todos los elementos que la componen, han llevado a las organizaciones a implementar medidas y controles que garanticen la integridad, confidencialidad y disponibilidad de su información y sus procesos asociados; es por esto, que los activos de información de cualquier empresa pública o privada, sin importar su tamaño o nicho de negocio, han evidenciado la necesidad de implementar sistemas integrados de gestión, para optimizar y garantizar la seguridad en la información y todos sus componentes asociados. Por otra parte, las organizaciones deben llevar a cabo evaluaciones y seguimientos (auditorías) periódicos, con la finalidad de tener una visión general de la implementación y conformidad de sus sistemas con la legislación, normas o regulaciones que describan las mejores prácticas de seguridad en la información. De igual modo, estas medidas son tomadas con el fin de minimizar la materialización de riesgos.

En este sentido, se han creado metodologías para la evaluación, seguimiento y revisión de los sistemas integrados de gestión, que garantizan el correcto desempeño y efectividad de los mismos, con el objetivo de estimular la mejora continua de los procesos; en este documento se describen los procedimientos necesarios para llevar a cabo una auditoría a sistemas de gestión de seguridad de la información, tomando como base las recomendaciones y lineamientos descritos en la norma internacional NTC ISO 19011 de 2012.

II. TIPOS DE AUDITORÍA

Antes de iniciar cualquier proceso de auditoría, es necesario aclarar que existen distintas clases o tipos; a continuación se hace una breve descripción de las mismas:

Tabla I.
Tipos de auditoría:

<table>
<tr><th rowspan="2">Auditoría Interna</th><th colspan="2">Auditoría Externa</th></tr>
<tr><td>Auditoría al proveedor</td><td>Auditorías de 3ra parte</td></tr>
<tr><td rowspan="2">A veces llamada auditoría de primera parte.</td><td rowspan="2">A veces llamada auditoría de segunda parte.</td><td>Para propósitos legales, regulatorios y similares.</td></tr>
<tr><td>Para certificación (ver también los requisitos en ISO/IEC 17021:2011)</td></tr>
</table>

Alcance de esta norma internacional y su relación con la norma ISO/IEC 17021:2011, NTC-ISO 19011 – Marzo de 2012.

Dando alcance a la tabla anterior, una auditoría interna de (primera parte), es aquella que se realiza al interior de una compañía, generalmente por personal de la misma organización; un ejemplo de este tipo de auditorías son las realizadas por la oficina de control interno. Una auditoría externa de (segunda parte), es la que realiza un cliente a sus proveedores, por ejemplo cuando un cliente realiza evaluaciones y seguimientos a sus proveedores de internet o canales de datos, a sus instalaciones y/o servicios, y una de (tercera parte), es la que realizan entidades certificadoras como la ISO, la certificación de un SGSI es un proceso mediante el cual una entidad de certificación externa, independiente y acreditada, audita el sistema, determinando su conformidad con la norma ISO/IEC 27001:2013, su grado de implantación real y su eficacia, y en caso de encontrar conformidad con la norma, emite el correspondiente certificado.

III. ENFOQUE DEL PROCESO

Uno de los cambios efectuados en la nueva versión de la norma ISO/IEC 27001:2013, fue la eliminación de la sección enfoque del proceso*;* se hace referencia del mismo en este documento, debido a que los sistemas de gestión como calidad y ambiental, que son correspondientes con la Norma de seguridad de la información ISO/IEC 27001:2013, siguen manteniendo esta sección y la norma NTC-ISO 19011:2012"directrices para la auditoria de los sistemas de gestión", establece que uno de los conocimientos y habilidades de un auditor son el "enfoque por procesos, análisis de procesos, técnicas de capacidad y control, métodos de tratamiento de riesgos…"[1]. De igual manera la ISO 27001.ES indica que "otra de las novedades es la eliminación del "enfoque a procesos" representado típicamente por el diagrama con el modelo "PDCA" característico hasta ahora en las publicaciones de los sistemas de gestión. ISO considera que el requisito fundamental es realmente la "mejora continua" y que podrían existir otras maneras alternativas al "enfoque a procesos" igualmente efectivas y aceptadas de alcanzarla aunque en cualquier caso sigue siendo este enfoque válido además de comúnmente aceptado" [2]. Es por esto que las metodologías y técnicas de auditoría del estándar ISO/IEC 27001:2005, establecen y promueven el enfoque por procesos para "establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI" [3]. En este sentido, un enfoque del proceso para la gestión de un SGSI requiere del monitoreo y revisión del desempeño y efectividad del SGSI y por lo tanto se incluye en este documento.

A. Modelo PHVA

Todos los modelos para la implementación de sistemas integrados de gestión como pueden ser de calidad, ambiental o el de nuestro objeto de estudio seguridad de la información, hacen uso de la metodología (planear, hacer, verificar y actuar - PHVA). A continuación se describe la metodología:

Figura I. Modelo PHVA - Estructura ISO/IEC 27001:2013, welivesecurity en español, Octubre de 2013.

Como se evidencia en la figura anterior, podemos enfatizar que las auditorías se posicionan en etapa del "verificar"; es allí donde los auditores de seguridad entran hacer su trabajo con el fin de evaluar el desempeño del SGSI. En este sentido el capítulo 9 (evaluación del desempeño) se definen las bases para medir la efectividad y desempeño del sistema de gestión a través de las auditorías internas y otras revisiones del SGSI, que plantean planes de acción que permitan atender y solucionar las no-conformidades [4].

IV. AUDITORÍA INTERNA DEL SGSI

Debido a que los sistemas de gestión son cambiantes en el tiempo, se hace necesario implementar metodologías de seguimiento y evaluación periódica como las auditorías internas, en las mismas se evalúa el cumplimiento de la implementación y operación de un SGSI. En la cláusula 6 de la Norma ISO/IEC 27001:2005 "auditorías internas SGSI", se enumeran los aspectos que los auditores deben tener en cuenta durante la realización de una auditoría de seguridad de la información, y también se anuncia la necesidad de realizar evaluaciones y seguimientos periódicos y planeados "la organización debe realizar auditorías internas SGSI a intervalos planeados para determinar los objetivos de control, controles, procesos y procedimientos del SGSI" [5]. En este sentido la norma ISO/IEC 17799 - 27002:2005, describe las actividades, requerimientos y aspectos a tener en cuenta a la hora de realizar una auditoría para evaluar un SGSI, con el fin de no entorpecer, interrumpir o retrasar los procesos que se llevan a cabo por la compañía o proceso auditado. A continuación se presentan los lineamientos de implementación:

a) Se debieran acordar los requerimientos de auditoría con la gerencia apropiada.

b) Se debiera acordar y controlar el alcance de los chequeos.

c) Los chequeos debieran limitarse a un acceso sólo-de-lectura al software y data.

d) Sólo se debiera permitir un acceso diferente al sólo-de-lectura para copias aisladas de los archivos del sistema, los cuales se pueden borrar cuando termina la auditoría, o se les puede dar la protección apropiada si existe la obligación de mantener dichos archivos en concordancia con los requerimientos de la documentación de auditoría.

e) Se debieran identificar explícitamente los recursos para realizar los chequeos y debieran estar disponibles.

f) Se debieran identificar y acordar los requerimientos de procesamiento especial o adicional.

g) Se debieran monitorear y registrar todos los accesos para producir un rastro de referencia; se debiera considerar el uso de rastros de referencia con la hora impresa para la data o sistemas críticos.

h) Se debieran documentar todos los procedimientos, requerimientos y responsabilidades.

i) La(s) personas(s) que llevan a cabo la auditoría debieran ser independientes a las actividades auditadas [6]. Cabe resaltar, que para la nueva versión ISO/IEC 27001:2013, el estándar ISO-27002 ya no es una referencia normativa, aunque continúa considerándose necesario en el desarrollo de la declaración de aplicabilidad (SOA, por sus siglas en inglés) [7].

V. DIRECTRICES PARA LA AUDITORÍA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

A. Principios de auditoría

Los principios de auditoría son características propias de un auditor y de su trabajo, los mismos, "deberían hacer de la auditoría una herramienta eficaz y fiable en apoyo de las políticas y controles de gestión, proporcionando información sobre la cual una organización puede actuar para mejorar su desempeño" [8]. Los principios por los cuales se debe regir un auditor a la hora de realizar su trabajo son (integridad, presentación imparcial, debido cuidado profesional, confidencialidad, independencia y enfoque basado en la evidencia) [9].

B. Programa de auditoría

Cualquier organización que lleve a cabo auditorias debería establecer un programas que "contribuya a la determinación de la eficacia del sistema de gestión del auditado"[10]. En el mismo se debe incluir las auditorías del SGSI que se requieran para evaluar su madurez o cumplimiento, y en este mismo sentido se sugiere que un programa de auditoría contenga como mínimo la siguiente información y recursos:

- Objetivos para el programa de auditoría y auditorías individuales.
- Alcance/número/tipos/duración/ubicación/cronograma de las auditorías.
- Procedimientos del programa de auditoría.
- Criterios de auditoría.
- Métodos de auditoría.
- Selección de equipos auditores.
- Recursos necesarios, incluyendo viajes y hospedaje.
- Procesos para manejo de confidencialidad, seguridad de la información, salud y seguridad y otros temas similares [11].

VI. REALIZACIÓN DE LA AUDITORÍA

A continuación se describen las actividades típicas que se deben realizar antes, durante y después de una auditoría:

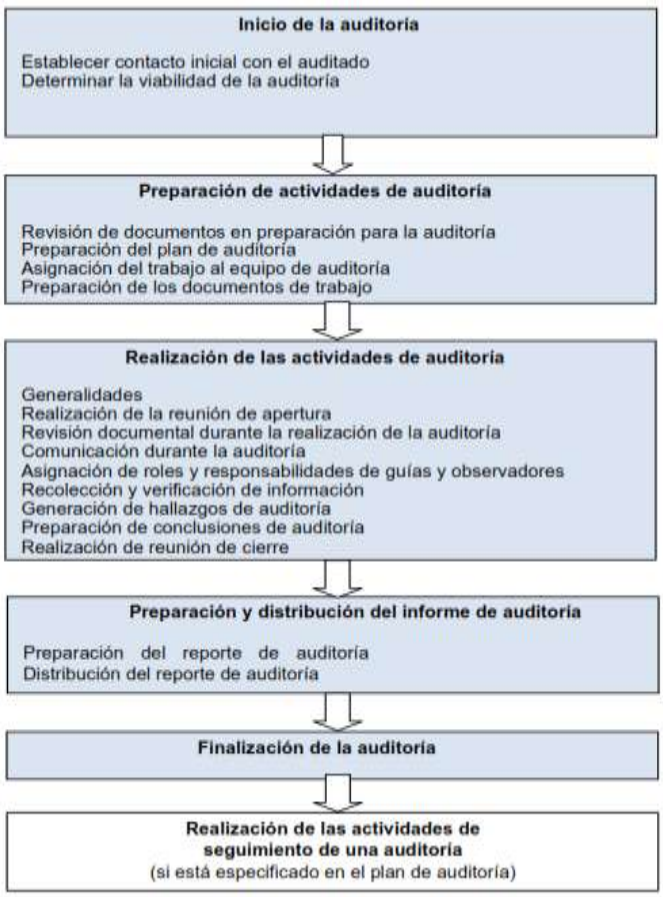

Figura II. Actividades típicas de auditoría, NTC-ISO 19011 – Marzo de 2012.

A continuación se hace una descripción de las tareas que se deben llevar a cabo en cada una de las fases de la auditoría, con el fin de llevar a buen término la misma.

A. Inicio de la auditoría

1) Establecer contacto inicial con el auditado

En esta fase se establece relación con el auditado, con el fin de:

- Establecer comunicación con los representantes del auditado.
- Confirmar la autoridad para la realización de la auditoría; — proveer información sobre los objetivos, alcance y métodos de auditoría, así como la composición del equipo auditor, incluyendo los expertos técnicos.
- Solicitar acceso a documentos y registros relevantes para propósitos de planeación.
- Determinar requisitos legales y contractuales aplicable y otros requisitos relevantes a las actividades y productos del auditado.
- Confirmar el acuerdo del auditado en lo referente al grado de divulgación y tratamiento de la información confidencial; — hacer arreglos para la auditoría, incluyendo la programación de fechas.

- Determinar cualquier requisito específico de la locación en cuanto a acceso, seguridad, salud y seguridad y otros.
- Llegar a acuerdos sobre la participación de observadores y la necesidad de guías para el equipo auditor.
- Determinar cualquier área de interés o inquietud del auditado en relación a la auditoría específica [12].

2) Determinación de la viabilidad de la auditoría

Esta tarea se basa en proporcionar la confianza suficiente al auditado, de que los objetivos de la auditoria son alcanzables. La determinación de la viabilidad tiene en cuenta factores como la disponibilidad de los siguientes recursos e información:

- Información suficiente y apropiada para la planeación y realización de la auditoría.
- Cooperación adecuada por parte del auditado.
- Tiempo y recursos adecuados para la realización de la auditoría [13].

B. Preparación de las actividades de auditoría

1) Realización de la revisión de la documentación en la preparación de la auditoría

Es necesario hacer una revisión exhaustiva de la documentación pertinente del SGSI, con el fin de reunir información relevante para preparar los papeles de trabajo (listas de verificación, entrevistas, etc.) como así también tener una visión general y global del SGSI, esta revisión preliminar le dará herramientas al auditor para detectar posibles falencias o carencias de documentación.

2) Preparación del plan de auditoría

Un plan de auditoría debe ser flexible para permitir los cambios que pueden hacerse mientras se lleva a cabo. El plan de auditoría debe contener y cubrir como mínimo los siguientes aspectos:

- Los objetivos de la auditoría.
- El alcance de auditoría, incluyendo la identificación de las unidades organizacionales y funcionales, así como los procesos a ser auditados.
- Los criterios de auditoría y cualquier documento de referencia.
- La ubicación, fechas, tiempo esperado y duración de las actividades de auditoría a realizar, incluyendo reuniones con la gerencia del auditado.
- Los métodos de auditoría a utilizar, incluyendo el grado de muestreo requerido para obtener suficiente evidencia de auditoría y el diseño del plan de muestreo, si aplica.
- Los roles y responsabilidades de los miembros del equipo auditor, así como de los guías y observadores.
- La adjudicación de recursos apropiados para áreas críticas de la auditoría [14].

3) Asignación de las tareas al equipo auditor

El líder del equipo de auditoría, debe asignar a cada miembro del equipo auditor las responsabilidades y tareas para auditar procesos, funciones, lugares, áreas o actividades específicos. Tales asignaciones deberían tener en cuenta la necesidad de independencia y competencia de los auditores, y el uso eficaz de los recursos, así como las diferentes funciones y responsabilidades de los auditores, auditores en formación y expertos técnicos. Se pueden realizar cambios en la asignación de tareas a medida que la auditoría se va llevando a cabo para asegurarse de que se cumplen los objetivos de la auditoría [15].

4) Preparación de los documentos de trabajo

Los documentos o papeles de trabajo, generalmente son una guía para el auditor, en los mismos se encuentran:

- Listas de verificación (checklist).
- Planes para la toma de muestras.
- Registros de asistencia.
- Actas de reunión, entre otros.

Estos papeles de trabajo se recomiendan que estén disponibles hasta que finalice la auditoría.

C. Realización de las actividades de auditoría

1) Realización de la reunión de apertura

En esta reunión se expone el plan de auditoría, con el fin de que el auditado si tiene alguna pregunta al respecto le sea resuelta antes de iniciar la misma, se recomienda que estén presentes: representantes de la dirección, los responsables del proceso a auditar y las partes interesadas, en general el propósito de la reunión es:

- Confirmar que todas las partes están de acuerdo con el plan de auditoría (auditado, equipo auditor).
- Presentar al equipo auditor.
- Asegurar que se pueden llevar a cabo todas las actividades de auditoría planeadas [16].

2) Realización de la revisión de la documentación durante la auditoría

La revisión de la documentación referente al SGSI permite determinar la conformidad del mismo contra los criterios de auditoría basados en la documentación disponible, esta misma información es el insumo que apoya las actividades de la auditoría. La revisión puede combinarse con otras actividades, siempre y cuando no se vea afectada la eficacia de la auditoría.

3) Comunicación durante la auditoría

Durante la auditoría se hace necesario establecer acuerdos de comunicación entre el equipo auditor y el auditado; el equipo auditor en cabeza del auditor líder, debe comunicar periódicamente el progreso de la auditoría y si es necesario resolver cualquier duda que tenga el auditado o cliente de auditoría. De igual manera se debe reportar cualquier cambio al plan de auditoría.

4) Recolección y verificación de la información

Una de las etapas más importantes de una auditoría es la recolección y verificación de la información, ya que es la única evidencia de conformidad frente a los criterios de auditoría, la información relevante a los objetivos, alcance

y criterios de la auditoría, incluyendo información relacionada con interfaces entre funciones, actividades y procesos debería ser recolectada por medio de muestreo apropiado y debería ser verificada. Solo información verificable debería ser aceptada como evidencia de auditoría. La evidencia de auditoría que conduce a hallazgos de auditoría debería ser registrada. Si durante la recolección de evidencia el equipo auditor conoce de circunstancias o riesgos nuevos o cambiantes, el equipo debería tratarlo en consecuencia [17].

A continuación se proporciona una visión general del proceso de recolección, análisis, verificación de la información pertinente y relacionada al SGSI o sistema objeto de revisión, la misma se expone hasta las conclusiones de la auditoría.

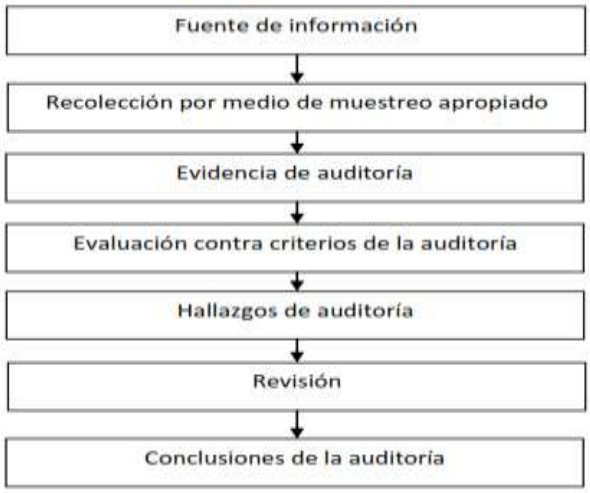

Figura III. Visión general del proceso de recolectar y verificar información, NTC-ISO 19011 – Marzo de 2012.

Los métodos de recolección de información incluyen (entrevistas, observaciones, revisión de documentos incluyendo registros).

5) Generación de hallazgos de la auditoría

La evidencia debe ser evaluada contra los criterios de la auditoría a fin de determinar los hallazgos, los mismos podrían indicar conformidad o no conformidad con los criterios de auditoría. Las no conformidades y su soporte (evidencia) deben ser registradas. Las no conformidades pueden estar clasificadas. Estas deberían ser revisadas con el auditado a fin de obtener reconocimiento de que la evidencia de auditoría es correcta y que las no conformidades son entendidas. Se debería realizar todo intento de resolver opiniones divergentes relacionadas con la evidencia o hallazgos de auditoría; cualquier punto sin resolver debería ser registrado [18].

6) Preparación de conclusiones de auditoría

El equipo auditor debería reunirse antes de la reunión de cierre con el fin de:

- Revisar los hallazgos de la auditoría y cualquier otra información apropiada recopilada durante la auditoría frente a los objetivos de la misma.
- Llegar a un acuerdo respecto a las conclusiones, teniendo en cuenta la incertidumbre inherente en el proceso de auditoría.
- Preparar recomendaciones, si esto está especificado en el plan de auditoría.
- Discutir el seguimiento a la auditoría, según sea aplicable. [19].

7) Realización de la reunión de cierre

El objetivo de esta reunión es presentar los hallazgos y las conclusiones de la auditoría. Los participantes deben ser generalmente los mismos de la reunión de apertura (dirección, responsables de los procesos o funciones auditadas y partes interesadas y por su puesto el equipo auditor). En esta reunión también se procura acordar los tiempos de implementación de los planes de acción por parte del auditado para erradicar las causas raíz de los hallazgos. Es recomendable redactar el acta de la reunión, con el fin de establecer los responsables y tiempos de la implementación de los planes de acción.

D. Preparación y distribución del informe de auditoría

1) Preparación del informe de auditoría

El líder del equipo auditor debería reportar los resultados de acuerdo con los procedimientos del programa de auditoría. El reporte de auditoría debería proveer un registro completo, exacto, conciso y claro de la auditoría y debería incluir o hacer referencia a lo siguiente:

- Los objetivos de la auditoría.
- El alcance de la auditoría, particularmente la identificación de las unidades de la organización y de las unidades funcionales o los procesos auditados.
- Identificación del cliente de auditoría.
- Identificación del equipo auditor y los participantes del auditado en la auditoría.
- Las fechas y los lugares donde se realizaron las actividades de auditoría.
- Los criterios de auditoría.
- Los hallazgos de la auditoría y la evidencia relacionada.
- Las conclusiones de la auditoría.
- Una declaración sobre el grado en el cual se han cumplido los criterios de la auditoría [20].

2) Distribución del informe de auditoría

El reporte de auditoría debería ser emitido dentro de un periodo de tiempo acordado. Encaso de demoras, las razones deberían ser comunicadas a la persona que gestiona el programa de auditoría.

El reporte de la auditoría debería estar fechado, revisado y aprobado, según aplique, de acuerdo con los procedimientos del programa de auditoría.

A continuación, el informe de la auditoría debería distribuirse a los receptores designados en los procedimientos o plan de auditoría [21].

E. Finalización de la auditoría

Una auditoria finaliza cuando se ha cumplido con todas las actividades planeadas.

La información, documentación y resultados de la auditoría solo pueden ser revelados a terceros salvo que sea requerido por ley, el equipo auditor y los responsables de la gestión del programa de auditoría no deberían revelar el contenido de los documentos, cualquier otra información obtenida durante la auditoría, ni el reporte de la auditoría a ninguna otra parte sin la aprobación explícita del cliente de la auditoría y, cuando sea apropiado, la del auditado. Si se requiere revelar el contenido de un documento de la auditoría, el cliente de la auditoría y el auditado deberían ser informados tan pronto como sea posible [22].

F. Realización de las actividades de seguimiento de una auditoría

Dependiendo de los objetivos de la auditoría, las conclusiones de la auditoría pueden indicar la necesidad de acciones correctivas, preventivas, o de mejora. Tales acciones generalmente son decididas y emprendidas por el auditado en un intervalo de tiempo acordado. Según sea apropiado, el auditado debería mantener informado a la persona que gestiona el programa de auditoría y al equipo auditor acerca del estatus de estas acciones.

La finalización y efectividad de estas acciones, debería ser verificada. Esta verificación puede ser parte de una auditoría posterior [23].

VII. CONCLUSIONES

Una auditoría está basada en la evidencia, por tal motivo es importante garantizar la integridad, confidencialidad y disponibilidad de la misma.

Durante la ejecución de una auditoría, es importante la revisión previa de los papeles de trabajo (listas de verificación, entrevistas, preguntas, etc.), paralelo a la revisión de la documentación, con el fin de no pasar nada por alto, y si hay inconsistencias que puedan conllevar a una no conformidad, la misma esté debidamente sustentada.

La realización periódica y oportuna de auditorías a los sistemas de gestión, brindan las herramientas necesarias para tomar decisiones estratégicas que contribuyen a la mejora continua de los procesos y al logro de los objetivos, misión y visión de una organización.

VIII. REFERENCIAS

[1] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act, Anexo A, Guía y ejemplos ilustrativos de conocimiento y habilidades de auditores específicas a una disciplina, Pág. 48.

[2] ISO 27001.ES – El Portal de ISO 27001 en Español – disponible en http://www.iso27000.es/certificacion.html#seccion4.

[3] International Organization for Standardization / International Electrotechnical Commission, ISO/IEC, "Tecnología de la información – Técnicas de Seguridad – Sistemas de Gestión de seguridad de la información – Requerimientos" ISO/IEC 27001:2005, 1era Ed, 2005, Pág. 5.

[4] welivesecurity en español - Publicada ISO 27000:2013, cambios en la norma para gestionar la seguridad de la información – disponible en http://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/.

[5] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act, Pág. 20.

[6] International Organization for Standardization / International Electrotechnical Commission, ISO/IEC, "Tecnología de la información – Técnicas de Seguridad – Sistemas de Gestión de seguridad de la información – Requerimientos" ISO/IEC 17799:2005, 2nd ed, 2005, Pág. 161 - 162.

[7] Magazcitum, El magazine para los profesionales de TI - ISO-27001:2013 ¿Qué hay de nuevo? – disponible en http://www.magazcitum.com.mx/?p=2397

[8] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, pág. 4

[9] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, pág. 4-5.

[10] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, pág. 4.

[11] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, pág. 6.

[12] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, pág. 19.

[13] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, pág. 19.

[14] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, pág. 20 – 21.
[15] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, Pág. 21.
[16] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, pág. 22.
[17] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, Pág. 25.
[18] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, Pág. 26.
[19] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, Pág. 26.
[20] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, Pág. 28.
[21] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, Pág. 29.
[22] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, Pág. 29.
[23] Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, "Compendio HSEQ (Directrices para la Auditoria de los Sistemas de Gestión)," NTC ISO 19011:2012, 1era Act. Bogotá: Icontec Internacional, Febrero de 2012, Pág. 29.

Autor

Johann Camilo Maldonado Peña
Ingeniero Electrónico
Aspirante a Especialista en Seguridad Informática
Certificaciones: FCNSA, FCNSP, Auditor Interno - HSEQ
Auditor de Seguridad Informática y de la Información en la Unidad Administrativa Especial de Catastro Distrital - UAECD
2015