**Universidad Mariano Gálvez**

**Maestría en Seguridad Informática**

Resumen ISO 19011

Auditoría informática

**21 de Enero de 2019**

1293-09-10116 Luis P. García Flores

# Introducción

En este documento voy a hacer un resumen sobre la ISO 19011. Esta norma establece las recomendaciones y la orientación para auditar los sistemas de gestión de una compania. Antes de empezar debemos saber que es un sistema de gestión y entender la importancia esta norma. Un sistema de gestión es un mecanismo que una organización utiliza para gestionar la documentación de cada uno de los procesos de la empresa.

En resumen, un sistema de gestión es un sistema para establecer políticas, objetivos y estándares para alcanzar dichos objetivos.El fin de implementar un sistema de gestión es **unificar la operación de todas las áreas del negocio** para alinearlas con los objetivos de la empresa. Es importante que **cada área tenga claro y definido tanto su objetivo como sus metas**. Esto da la garantía de direccionar tu negocio más fácil y eficazmente.

Ahora, ya que tenemos una idea general sobre que es un sistema de gestión vamos a enfocarnos en la ISO 19011 que se encarga de auditarlo.

ISO 19011 es una norma internacional desarrollada por la Organización Internacional de Normalización, que establece las directrices para la auditoría de los sistemas de gestión de la calidad. La última revisión de la norma fue en julio de 2018.

Esta norma internacional proporciona orientación sobre la auditoría de los sistemas de gestión, incluyendo los principios de la auditoría, la gestión de un programa de auditoría y la realización de auditorías de sistemas de gestión, así como orientación sobre la evaluación de la competencia de los individuos que participan en el proceso de auditoría.

La norma ISO 19011 no establece ningún tipo de requisito específico, sino que sirve de guía para la gestión del programa de auditorías, así como para la planeación y realización de las mismas, junto con las competencias y evaluación del equipo auditor.

# Resumen de ISO-19011

Según lo establecido en esta ISO, se pretende brindar una orientación, no requerimientos. Dichas directrices pueden diferir de acuerdo con el tamaño, la naturaleza y la complejidad de las organizaciones quese van a auditar, así como con los objetivos y alcances de las auditorías que se vayan a realizar.

En esta ISO se proporciona además, ejemplos para casos específicos, conceptualizaciones y una guía sobre los procesos de programación y planificación de auditorías. Esta ISO resalta lo importante de las auditorias, por cuanto la gerencia sin la práctica de una auditoria no tiene plena seguridad de que los datos que estánsiendo registrados realmente son verdaderos y confiables. Es la auditoria que define con bastante razonabilidad, la situación real de la empresa.

Puede evaluar, por ejemplo, los estados contables en su conjunto o una parte de ellos, el correcto uso de los recursos humanos en la compania, el uso de los materiales y equipos y su distribución, etc. Contribuyendo con la gerencia para una adecuada toma de decisiones, logrando así las metas fijadas por el staff.

En este resumen quiero resaltar estos 3 puntos que explican los aspectos principales de una auditoría de sistema de gestión, es posible que estos mismos aspectos puedan ser aplicados perfectamente al momento de auditar otra clase de sistemas.

**Una auditoria además, evalúa el grado de eficiencia y eficacia con que se desarrollan las tareas administrativas y el grado de cumplimiento de los planes y orientaciones de la gerencia.**

**Debemos tener claro que la auditoría debe estar basada en objetivos definidos por el cliente.**

**El alcance de la auditoría es determinado por el auditor líder en acuerdo con el cliente para alcanzar los objetivos.**

El alcance de una auditoría describe **la extensión y límites de la auditoría**, y abarca todo el sistema de gestión de calidad, procedimientos, y de todos los apartados de la norma decalidad aplicada para la implantación del sistema así como la información relativa a documentación legal y administrativa de la empresa por el equipo auditor, enfactores tales como la ubicación física, actividades organizacionales, y la forma de realizar los informes.

La auditoría se caracteriza por depender de diferentes principios. Los principios tienen que ayudar a realizar la auditoría, es decir, proporcionan herramientas eficientes y fiables de apoyo a las políticas y controles de gestión, facilitando información sobre cómo debe actuar una organización para mejorar su desempeño.

Adherirse a los principios es un requisito previo para establecer las conclusiones de la auditoría que sean pertinentes y suficientes y permiten que los auditores trabajen independiente para conseguir conclusiones similares en circunstancias similares.

La ISO 19011 tiene 6 principios de auditoría que, como bien escribí al inicio del documento, no tiene requisitos explicitos, sino recomendaciones y orientación a la organización. Voy a describir de manera general pero precisa los 6 principios de auditoría de la ISO 19011:

**Integridad:** es una base clara de responsabilidad profesional. Los responsables de la gestión de un programa de auditoría y los auditores deben desempeñar su trabajo con honestidad, responsabilidad, observar y cumplir todos los requisitos legales a los que estén sujetos, desarrollar su trabajo de forma imparcial, demostrar la competencia a la hora de realizar su trabajo, es decir, sin estar influenciados por nada y por nadie. Debe ser insensible hacia cualquier influencia externa que pueda ejercer su juicio mientras realiza una auditoría.

**Presentación imparcial:** es ser transparente e informar con exactitud y veracidad. Todos los hallazgos, conclusiones e informes tienen que reflejar claramente y con exactitud todas las actividades que se realizan durante las auditorías. Todos los obstáculos que se encuentran en el camino al realizar la auditoría deben ser informados, al igual que las opiniones divergentes que se queden sin resolver entre el equipo auditor y la persona auditada. La comunicación entre los interesados tiene que ser transparente, exacta, objetiva, oportuna, sincera y útil.

**Ser profesional:** tener un juicio de experto al realizar la auditoría. Cada auditor debe ser precavido y tener cautela, la confianza que se deposite en ellos por el cliente de la auditoría y por las demás partes interesadas según la importancia que tenga la tarea que quieren desempeñar. Un gran factor a tener en cuenta a la hora de realizar su trabajo con el debido cuidado profesional es contar con la capacidad de realizar juicios de expertos razonados con evidencia que respalde sus conclusiones, esto es aplicable con todas las situaciones de la auditoría.

**Confidencialidad:** toda la información utilizada debe ser cuidada y protegida según su importancia. Los auditores deben cumplir con un acuerdo de discreción durante la utilización y la protección de la información que el cliente le ha proporcionado y que ha adquirido durante la ejecución de la auditoría. El concepto incluye el uso y aplicación apropiada de la información sensible o confidencial de la organización. La información de la auditoría no puede usarse de para beneficio personal del auditor o del cliente de la auditoría, de forma que pueda perjudicar al interés legítimo del auditado o del auditor.

**Independiente:** para que una auditoria sea imparcial y la objetividad de las conclusiones de la auditoría tengan validez debe existir independencia. En pocas palabras, los auditores no pueden ser juez y parte en asuntos de auditoria. Los auditores deben ser ajenos a la actividad que se quiere auditar siempre y cuando sea posible, para que tenga credibilidad. Pueden existir casos en los que deben actuar de forma libre, y un conflicto de intereses es lo que menos se espera. Para las auditorías internas, se recomienda los auditores vengan de otro departamento o area, que no tenga relación directa de entrada o salida hacia el proceso que van a auditar.

Los auditores deben mantener la claridad según el proceso de auditoría para asegurarse de los hallazgos y las conclusiones de la auditoría que se basan sólo en la evidencia de la auditoría. No importa el tamaño de la empresa, siempre debe lucharse por la independencia de procesos entre auditor y auditado.

**Enfoque basado en la evidencia:** Aspecto clave para obtener conclusiones respaldadas, que sean fiables, que puedan reproducirse y tengan un valor en un sistema de auditoría. Toda la evidencia encontrada en una auditoría debe ser verificable. Regularmente se usa la información que se tiene disponible por parte del auditor, ya que la auditoría se realiza durante un tiempo muy limitado comaparado con el tiempo de ejecución del proceso. Debe existir un proceso correcto para muestrear, ya que podría poner en riesgo la confianza de las conclusiones.