UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica

Universitat Politècnica de València

Las normas de gestión de empresas y su aplicación a las empresas informáticas. La auditoría y la certificación de empresas

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Adrián Martínez Rochina

Tutor: Mariluz Gordo Monzó

Curso 2018/2019

Resumen

Las normas de gestión son muy importantes para todo tipo de organizaciones, aportan gran cantidad de información, que le sirve a la empresa para tener un futuro con mayor éxito. Estas normas son realizadas por expertos de los diferentes sectores (organizaciones que investigan, los consumidores, sector gubernamental…), y están respaldadas por la entidad ISO (International Standarization Organization), que es la encargada de implantar una serie de normas de fabricación, comercio, comunicación y gestión. En este trabajo veremos el uso de tres series de normas de gestión diferentes que se pueden aplicar en empresas informáticas, estas son la ISO 9000, ISO 27000 e ISO 20000. Asimismo veremos cómo implementar una norma de gestión, los pasos que una organización ha de seguir para conseguir los diferentes certificados y los beneficios que obtendrán las empresas al estar certificadas. Para realizar el seguimiento de que se cumplen estas normas, la auditoría interna es un factor muy importante en la parte de la implementación y la auditoría externa en el apartado de la certificación, es aquí donde tenemos a la figura del auditor.

Palabras clave: normas de gestión, ISO, auditor, certificado.

Resum

Les normes de gestió són molt importants per a tot tipus d'organitzacions, aporten gran quantitat d'informació, que necessiten les empreses per a tindre un futur en major èxit. Estes normes són realitzades per experts dels diferents sectors (organitzacions que investiguen, els consumidors, sector gubernamental...), i estàn recolzades per l'entitat ISO (International Standarization Organization), que és l'encarregada d'implantar una sèrie de normes de fabricació, comerç, comunicació i gestió. En este treball vorem l'ús de tres sèries de normes de gestió diferents que es poden aplicar en empreses informàtiques, estes són la ISO 9000, ISO 27000 i ISO 20000. Aixina mateix vorem com implementar una norma de gestió, els passos que una organització ha de seguir per aconseguir els diferents certificats i els beneficis que obtindràn les empreses al estar certificades. Per a realitzar el seguiment de que s'acompleixen estes normes, l'auditoria interna és un factor molt important de la part d'implementació i l'auditoria externa en la part de certificació, és ací on apareix la figura de l'auditor.

Paraules clau: normes de gestió, ISO, auditor, certificat.

Abstract

The management standards are very important for all kind of organizations, they give us a big quantity of information, this type of information is what the companies need to have a successful future. These standards have been made by experts from different sectors (organizations that investigate, the consumers, government sector...), and they are supported by the entity ISO (International Standardization Organization), which is the responsable to set standards series of manufacturing, trade, communication and management. In this project we'll see the use of three differents management standards that we can apply to IT companies, these series are the ISO 9000, ISO 27000 and ISO 20000. Furthermore we'll see how to set a management standard, the steps that a organization has to follow for achieving the different certificates and the benefits that they will obtain when they get the certificate. So to track that this standards are fulfilled, the internal audit is a really important factor on the setting part and the external audit on the certificate part, it's here where we have the auditor.

Keywords : management standards, ISO, auditor, certificate.

Tabla de contenidos

1. Introducción

Las normas de gestión resultan imprescindibles para todo tipo de empresas, ya que nos aportan conocimientos de una forma explícita, ayudando a las organizaciones a ser más innovadoras y productivas tanto internamente, dentro de la organización, como externamente. Las normas de gestión son aquellas que van a ayudar a gestionar de una manera eficaz y eficiente la organización. Estas normas están sujetas a sistemas de gestión, los cuales son un conjunto de reglas que contribuyen a la gestión de procesos en una organización y va a permitir establecer unos objetivos, una política y poder alcanzar dichos objetivos.

Existen diferentes series de normas de gestión, cada una de ellas nos aportan beneficios para la mejora continua de la empresa, planificando objetivos de mejora y realizando un seguimiento de los mismos, así como teniendo en cuenta las no conformidades y las reclamaciones de los clientes, que deben de servir para identificar puntos débiles en la organización o elementos a mejorar en la misma. Por lo que, certificarnos de la mayor cantidad de normas posibles nos aportará un mayor grado de prestigio, tanto en mercados nacionales como internacionales, no solo es este el objetivo de las empresas a la hora de certificarse en cualquiera de las normas reseñadas, sino disponer de un mayor conocimiento de todo el sistema productivo y saber identificar sus deficiencias y oportunidades, así como identificar posibles riesgos. Para poder solventar estos problemas haremos uso de la auditoría interna, que es aquella que va a ayudar a la organización a implementarse de una norma. La implementación de una norma ISO es un gran paso hacia la certificación y gracias a este proceso, se tendrá en la organización una norma correctamente instaurada y haciendo buen uso de los beneficios que aportará. Posteriormente al proceso de la auditoría interna, se podrá realizar la auditoría externa para buscar el certificado, el cual dará a la empresa un mayor prestigio a un nivel más internacional, con los clientes y nos ayudará a ser más competitivo. Nos centraremos más en aquellas normas de gestión que involucran a empresas TICS (tecnologías de la información y comunicaciones), según “la Organización internacional de la estandarización” en este sector las más populares que encontramos son la ISO 9000 basada en la gestión de la calidad, la ISO 27000 basada en la seguridad de los datos y la ISO 20000 basada en la gestión de servicios, las cuales se explicarán en este proyecto.

En estas normas se certifican gran cantidad de empresas cada año, en la guía que se ha realizado en este proyecto se verán las pautas básicas que hay que tener en cuenta para instaurar estas normas en una empresa y los beneficios que tendremos al realizarlo, además del proceso de certificación que se tendrá que seguir.

1.1 Motivación

Actualmente cualquier empresa tiene un certificado ISO y si no lo tiene es posible que tenga implementada una de las normas, por lo que es un tema bastante importante si se

busca una mejora continua en una organización. Este TFG está destinado a conocer estas tres normas ISO, al estudio de la implementación y posteriormente de la certificación, ya que es algo que está en continua actualización y es interesante conocer.

Principalmente este tema es interesante de tratar debido a la importancia que tienen hoy en día las normas de gestión, y es por ello que se quiere recopilar toda la información que se cree oportuna para plasmarla en este documento, acerca de las normas de gestión que se han considerado más importantes para las empresas TICs y resolver para las empresas no certificadas cualquier duda que puedan tener durante el proceso de implementación y certificación, explicando los puntos que hay que seguir para alcanzar el objetivo. Estas normas contribuyen al mundo en que vivimos, facilitandonos el comercio, difundiendo conocimiento, realizando avances innovadores en tecnología y comparten buenas prácticas de gestión y conformidad.

Si hablamos de las normas de gestión no podemos pasar por alto la serie de normas ISO 9000 de gestión de calidad ya que es una de las más importantes y una de las que más reconocimiento tiene en la actualidad y es la que nos aportará un mayor nivel de calidad a nuestra empresa. Al igual pasa con la serie de normas ISO 27000 basada en la gestión de la seguridad de la información, esta norma en los últimos años está siendo una de las más importantes sobretodo en el sector de las tecnologías de la información ya que, en la actualidad muchas organizaciones buscan la seguridad de los datos y que no salga información importante a la luz, si esto llegara a pasar nuestros competidores se verían altamente beneficiados y nuestra organización a su vez empequeñecida. Mientras que la serie de normas ISO 20000 trata sobre la gestión de los servicios de las tecnologías de la información.

Importante es también el papel del auditor, para comprobar que se cumplen correctamente las condiciones para poder implementar una norma, realizando la auditoría interna o poder certificarse mediante la auditoría externa, se seguirán una serie de pautas para comprobar que todo esté correcto y funciona de acuerdo a la norma. El proceso de certificación puede resultar extenso y pueden surgir inconvenientes a la hora de realizar la implementación de la norma. Cómo conseguir la certificación está correctamente explicado en la guía con todas las pautas a realizar.

El papel que tiene el consultor es ayudar a la hora de mejorar la organización para que pueda ser instaurada la norma y sea más fácil de pasar el proceso de auditoría interna. Este proceso de mejora lo podría realizar un grupo de personas de la propia empresa. aunque probablemente resulte más eficaz y eficiente delegar esta responsabilidad en un profesional como es el consultor, este va a sugerir los cambios para mejorar a la organización y cómo realizar los mismos.

El papel del informático con responsabilidad dentro de la organización va ser muy importante para que la norma implantada o que se va a implantar funcione. En el proceso en el que la norma se va a implementar este tendrá que contestar cualquier duda que pueda tener el consultor, el grupo de personas o el propio auditor que quieran saber el funcionamiento de los sistemas informáticos de la organización. También hay que tener en cuenta que estos informáticos tendrán la responsabilidad de mantener en correcto orden el funcionamiento de estas normativas, como puede ser en el caso de las ISO 27000 manteniendo la seguridad de la información de la empresa y que esta información no pueda llegar hasta nuestros principales competidores.

1.2 Objetivos

Se va a elaborar una guía, con información sobre las tres normas indicadas anteriormente, orientada a empresas del ámbito de las tecnologías de la información y comunicaciones, para aportarles información y hacerles el camino un poco más fácil, guiándolas en el proceso de implementación, paso a paso, e indicando el procedimiento para finalmente certificarse, explicando la auditoría y el papel del auditor. El objetivo es dar respuesta a esta serie de preguntas:

1. ¿Qué es una norma de gestión y quién las certifica?
2. ¿En qué consiste la norma de gestión ISO 9000:2015. Sistemas de gestión de calidad?
3. ¿En qué consiste la norma de gestión ISO 20000:2018. Tecnologías de la información (TI). Gestión de los servicios?
4. ¿En qué consiste la norma de gestión ISO 27000:2019. Sistemas de gestión de la seguridad de la información?
5. ¿Qué es la auditoría?
6. ¿En qué consiste el proceso de implementación y auditoría interna?
7. ¿Cómo conseguir la certificación?
8. ¿Qué cantidad de empresas se certifican en cada normativa de las anteriormente señaladas?
9. ¿Cuál es el coste de certificación?
10. ¿Qué cuentan las empresas certificadas?

1.3 Impacto esperado

Cualquier persona puede ir a buscar información en Internet acerca de las normas de gestión, implementación y certificación, pero se va a encontrar con documentos extremadamente extensos y a veces incluso tediosos a la hora de leerlos, por lo que se trata de identificar lo más importante que cualquier empresa debería de tener en cuenta, de las encuestas realizadas y conversación telefónica con alguna de ellas, se ha podido determinar en qué puntos, tuvieron mayores dificultades al implementar las tres normas, lo cual ha servido como orientación a la hora de realizar la presente guía. Se han realizado trabajos de investigación, una entrevista a un gerente de una empresa del sector de las tecnologías de la información y comunicaciones y se enviaron encuestas. Por lo que se va a obtener información de una situación real que ha tenido una empresa, con los beneficios y problemas que han tenido las propias empresas al certificarse o implementar una de estas normas en su organización.

En toda la información buscada en otros trabajos no se ha encontrado información del conjunto de las normas de gestión de las que se va a hablar en este proyecto en un mismo trabajo, por eso es novedoso y hay pocos TFGs en gestión y este lo es.

Esta guía pretende ser un documento de fácil lectura y seguimiento para cualquier empresa que no conozca las normas de gestión, ayudándole a identificar las ventajas que para su organización obtendría la implementación e incluso posterior certificación de las mismas.

1.4 Metodología

Los pasos que se van a seguir para cumplir con lo dicho anteriormente será, una investigación de las normas de gestión que puedan ser aplicables a empresas TICS en iso.org y Aenor, y ver cuáles han sido las más certificadas y podrían ser útiles para este tipo de organizaciones, también se buscarán estadísticas en empresas certificadoras de las normativas en cuestión ISO.

Se realizará un estudio de investigación de la serie de normas ISO 9000, ISO 20000 e ISO 27000 con el fin de comprender su funcionamiento, como se implementan y ventajas que nos aportarán. Tras la fase de implementación, si la empresa busca la certificación, seguiremos con la explicación de este proceso con los pasos que se tendrán que seguir para conseguirla, y las ventajas que nos proporcionará el hecho de adquirir el certificado. También haremos uso de Riunet, Google Académico, Teseo y Polibuscador para obtener en artículos, libros y trabajos académicos diferente información relacionada con las normas, su implementación y la certificación.

Se enviarán varias encuestas a organizaciones del sector de las tecnologías de la información y comunicaciones, basadas en la implementación y certificación de estas tres normas, para comprobar de primera mano las respuestas que obtenemos de empresas del sector. Se realizará una entrevista a una empresa del sector TIC, para comprobar las dudas que pueda tener una organización no certificada a la hora de afrontar el proceso de implementación o certificación de una norma. El resultado que se espera de la entrevista, es recopilar información sobre los puntos en los cuales puedan tener algún tipo de problema y resolverlos en la guía. La entrevista ha aportado gran valor en algunos puntos de la guía, como la explicación del proceso de implementación o el coste de certificación, entre otros.

Se realizarán llamadas a varias certificadoras para conocer el precio de certificación de estas tres normas. El resultado de estas llamadas queda reflejado en la guía y se puede comprobar, cómo dependiendo de la organización los precios variarán en función de los días que dediquen a la realización de la auditoría externa, el cálculo de los días necesarios para la realización de la auditoría externa irá en función del número de trabajadores de la organización y de la complejidad de la misma.

1.5 Estructura

Capítulo 2

Estado del arte y crítica. Se analizará la información que ya existe sobre el tema que se va a tratar, esta información se ha encontrado mediante los siguientes medios: Riunet, Google Académico, Teseo y Polibuscador. A los trabajos relacionados con el presente TFG se les realizará una pequeña crítica y se explicará en que completa este trabajo a otros ya existentes o en que los mejora.

Capítulo 3

Análisis del problema. En este punto se va a analizar las oportunidades de negocio del proyecto y se tendrá en cuenta el proyecto de la guía realizada como ayuda para las organizaciones que se quieran certificar y/o entender de las tres normas anteriormente comentadas.

Capítulo 4

Diseño de la solución propuesta. Se hablará del formato que se ha elegido para la solución y también se hablará de forma resumida del índice que encontramos en la solución propuesta.

Capítulo 5

Desarrollo de la solución propuesta. Se hablará del producto final que es la guía y los problemas que se han tenido para redactarla y para conseguir la información necesaria para completarla correctamente.

Capítulo 6

Conclusiones. En este capítulo se presentan las principales conclusiones obtenidas después de la realización del proyecto.

Capítulo 7

Trabajos futuros. En este capítulo se presentarán las posibles opciones que se podrán realizar para mejorar de alguna forma la solución final del proyecto.

Capítulo 8

Referencias. Se podrán ver las fuentes de información usadas para la realización del proyecto.

Capítulo 9

Anexo. En este capítulo encontraremos la solución del proyecto, la guía.

2. Estado del arte y crítica

En este punto se va tratar los trabajos ya existentes de este tema, qué información podemos encontrar y qué nos va a aportar este trabajo que no nos hayan aportado estos proyectos ya existentes.

En general y como bien se ha dicho en el punto anterior, existe un gran volumen de información de todas las normas de gestión, por eso en este trabajo se va a tratar de seleccionar las tres más interesantes para las empresas TICS y aportar la información que se ha creído necesaria para el interés de las organizaciones del sector.

Según la investigación realizada entrando en sitios como Riunet, Teseo y en Google académico se ha encontrado información de alguna norma de gestión en concreto, pero no se ha encontrado ningún proyecto donde se hable de tres diferentes normas de gestión, sino que se suele concretar en una o dos y aporta la mayor información posible de esta o estas normas, o aplica una norma en concreto a una empresa, por eso, este proyecto es novedoso, ya que se va a hablar de varias normas que se pueden aplicar en este caso a empresas TICS, en concreto se hablarán de las tres normas de gestión que se han considerado más importantes o que más puedan aportar a este tipo de organizaciones. Estos trabajos ya existentes nos aportan una conclusión clara de que las normas de gestión aportan grandes beneficios competitivos para las empresas y nos ayudan a conseguir una mayor eficiencia y eficacia. A continuación se muestran algunos de los diferentes trabajos o artículos y donde se han podido encontrar, junto con un pequeño resumen del contenido del mismo:

MEDIO	**Autor y documentación**	**ISO9000**	**ISO20000**	**ISO27000**
Riunet	Autor: Jorge Anduix Fuentes. Año:2015. Trabajo final de grado.			El trabajo nos expone lo que tenemos que tener en cuenta si queremos instaurar la norma ISO 27001 en una empresa TIC. Analizando la empresa y su SGSI y establecer un nuevo SGSI para tener una mayor protección de datos.

MEDIO	Autor y documentación	ISO9000	ISO20000	ISO27000
Google académico	Autor: Lourdes Aja Quiroga. Año: 2002. Revista SciELO Analytics Título: Gestión del conocimiento, gestión de información y gestión de la calidad en las organizaciones	Artículo que nos habla acerca de la evolución de la tecnología y la importancia que tiene para las empresas, donde podemos ver información acerca de la gestión de la información, gestión del conocimiento y gestión de calidad y la importancia de cada una de ellas.		
Google académico	Autor: Janett Yánez y Raiza Yánez. Año:2012. Red de revistas Redalyc. Título: Auditorías, Mejora Continua y Normas ISO: factores clave para la evolución de las organizaciones.	Busca la mejora continua mediante la norma ISO 9000 y nos explica acerca de ella, también se centra en la investigación de analizar los fundamentos y la auditoría.		
Teseo	Autor: Arturo Ugalde Canitrot. Año: 2015. Tesis doctoral.	Se centra en el campo de la epileptología, analizando las consecuencias de la aplicación de un sistema de gestión de calidad en el Laboratorio de Monitorización de Video-EEG.		
Riunet	Autor: Raúl Francisco Oltra Badenes. Año: 2017		Nos explica para que nos va a servir la ISO 20000, su historia, los beneficios que obtendrá nuestra organización al implantar y certificar de esta norma y su contenido.	

2.1 Crítica al estado del arte

Durante esta investigación de proyectos se encontraron trabajos realizados por exalumnos de la ETSINF como se ha visto en el apartado anterior, en uno de ellos se exponía de una manera muy clara la implantación de la ISO 27001 en una empresa del sector, pero no explica el proceso que hay que seguir después de la implementación para conseguir la certificación. Hubiese sido más completo el haber acabado el proyecto realizando una explicación del proceso de certificación. No se habla de ninguna otra normativa de las que se van a hablar en este proyecto.

El artículo de Lourdes Aja Quiroga habla de forma más teórica acerca de la ISO 9000 pero en ningún momento nos da información acerca de la implementación de esta, ni de la certificación de la ISO 9001, se basa en la explicación de las normas que componen la familia ISO 9000, por lo tanto, faltaría algo más de información acerca de la implementación de esta norma. No se habla de ninguna otra normativa de las que se van a hablar en este proyecto.

El siguiente artículo de Google académico de Janett Yánez y Raiza Yánez nos va a dar la importancia de la norma ISO 9000 y cómo vamos a lograr la mejora continua mediante las auditorías. En este caso sí que comenta el proceso que hay que seguir para adquirir el certificado, primero con la auditoría interna y más tarde cuando se ha pasado el proceso de implementación conseguir el certificado con la auditoría externa. Pero sigue sin aportarnos más normativas del sector de las tecnologías de la información de las que se van a hablar en este proyecto, en la presente guía.

La tesis doctoral implementa la norma ISO 9001 en un laboratorio de monitorización de video-EEG, informándonos de lo más importante a tener en cuenta de esta norma y del proceso que ha seguido para realizar esta complicada implementación. Aunque se expone muy bien todo lo relacionado con el sistema de gestión de calidad, pasa exactamente igual que en el caso anterior, y es que no hace referencia a las normas comentadas anteriormente y es lo que le diferencia del presente proyecto.

Por último en el documento basado en la ISO 20000, donde se realiza una explicación de la historia, de para qué va a ayudar esta serie de normas y los beneficios que va a aportar implementarnos y certificarnos de ella. No indica cómo se puede conseguir la implantación y la certificación de esta norma.

Se ha realizado una minuciosa investigación encontrando varios trabajos, artículos y capítulos de libros similares a lo anteriormente comentado. Se puede concluir, que se pueden encontrar proyectos que hablen de algún tema relacionado con este trabajo pero no que exponga este trabajo en todo su conjunto.

2.2 Propuesta

Lo que este proyecto nos va a proporcionar, que no podemos encontrar en ningún otro trabajo, es una explicación clara acerca de las tres normas de gestión que se han considerado más importantes para las empresas TICS, los pasos que hay que seguir para su implantación, el proceso de auditoría que se tendrá que llevar a cabo para lograr el certificado, los beneficios que nos aportará el implementarnos y lograr el certificado de cada una de estas normativas.

Realizando una guía para entender todo lo anteriormente dicho y que ayude a las empresas del sector a entender acerca de estas normas y del proceso de implantación y certificación. Hay empresas que no tienen ningún certificado y la idea es que esta guía les solucione cualquier duda que les pueda surgir.

3. Análisis del problema

Este trabajo va a brindar información a las empresas del ámbito de las TICs sin experiencia en las normas ISO, pero con inquietudes sobre estas, con el fin de facilitarles el acceso a las mismas y que les solucionen las dudas que puedan encontrar acerca de su funcionamiento, mediante los próximos puntos del trabajo se pretenderá abordar los problemas que pueda tener el lector sobre las propuestas realizadas anteriormente, que se irán concretando a lo largo del trabajo.

3.1 Marco legal y ético

En este punto hablaremos de la legislación vinculada a la información de las tres normas y del marco ético.

MARCO LEGAL

ISO 27001. Sistemas de gestión de la seguridad de la información y 20000-1. Tecnologías de la información (TI). Gestión de los servicios

Para implementar un sistema de gestión de la seguridad de la información según la norma de gestión ISO 27001 y de gestión de los servicios de la tecnología de la información, norma de gestión ISO 20000-1, se deben de considerar como requisitos legales los relacionados a continuación:

- **Ley de Propiedad Intelectual 1/1996 del 12 de Abril de 1996:** La propiedad intelectual protege los derechos de autores, artistas, productores y organismos de difusión, respecto a las obras originales de su creación. Comprende los siguientes derechos: Derechos morales, derechos patrimoniales y derechos a solicitar compensación económica por la explotación de la obra.

- **Ley Orgánica de Protección de Datos (LOPD) de carácter personal 3/2018 del 5 de Diciembre de 2018:** El objeto principal de la LOPD es adaptar el ordenamiento jurídico español al reglamento de la Unión Europea en lo relativo al tratamiento de datos personales y la libre circulación de los mismos, a la vez que se garantizan los derechos digitales de la ciudadanía establecidos en el artículo 18.4 de la Constitución. Dentro de los derechos digitales se hace especial hincapié al derecho de los usuarios a la seguridad de las comunicaciones a través de Internet, la protección de los menores en Internet, derechos de rectificación en Internet, derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, derecho al olvido en búsquedas de Internet y redes sociales.

- **Ley de servicios de la sociedad de la información y comercio electrónico 34/2002 del 11 de Julio de 2002:** Esta ley establece las reglas que deben cumplir los proveedores de servicios de intermediación, empresas que ofrecen sus productos en Internet y a los ciudadanos que poseen una página web, así como la actividad económica que se pueda generar en la compra y venta de productos y servicios que sea de forma segura y confiable.

- **Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo del 6 de Julio de 2016:** Cuyo objetivo es establecer una serie de medidas que garanticen un buen nivel de seguridad de los sistemas y redes de la Unión Europea. Esta directiva surge debido al hecho de que un ciberataque presenta una gran amenaza a los sistemas de información y de las redes. Se pretende, que esta nueva medida de ciberseguridad los proteja.

ISO 9001:2015. Sistemas de gestión de calidad

En este caso hablaremos de la ISO 9001 la cual no tiene una legislación concreta pero dependerá del producto o servicio que realice la organización.

MARCO ÉTICO

En cuanto a la ética, es muy importante que todos los implicados en el sistema de gestión conozcan los requisitos legales y normativa vigente, por ejemplo, conocer la ley orgánica de protección de datos con el fin de evitar filtración de información. Especial importancia tiene la figura del auditor por su objetividad y ética a la hora de realizar las auditorías. El auditor debe demostrar profesionalidad en todas las acciones realizadas en el proceso de auditoría, documentando todas las conclusiones que extraiga de la empresa a la que audita.
En el caso de la figura del informático, tiene acceso a mucha información que deberá de gestionar con profesionalidad y haciendo un buen uso del sistema de seguridad de la información, para que los datos de terceros o de la propia empresa sigan siendo confidenciales para el resto del mundo.
Aunque las personas son las que tienen que hacer buen uso de las normativas, son también las que producen fallos como puede ser el siguiente caso basado en la norma de gestión ISO 27001:

- El caso de la brecha de seguridad de Yahoo!: La compañía tuvo una fuga de datos y alrededor de 500 millones de clientes comprobaron que sus datos se podían conseguir en Internet.

3.2 Análisis de riesgos

En este punto se van a analizar los posibles riesgos que puede encontrar una organización y los riesgos que puede tener la guía creada.
Los principales riesgo que puede tener una organización son:

- Podemos encontrar empresas que por su deficiente gestión de la información

corran el riesgo de pérdida de la misma o que esta pueda ser publicada afectando a terceros. Es el caso del problema comentado anteriormente de la brecha de seguridad de Yahoo!, a partir de una mala gestión de la seguridad de la información, se produjo un ciberataque y los datos de las personas fueron publicados en Internet. Como solución para estas empresas con una buena implementación en la normativa de gestión ISO 27001 y siguiendo las pautas de las mismas evitarían en gran medida las fugas de la información.

- Otro tipo de empresas que podemos encontrar, son aquellas que no van a resultar competitivas dentro del sector por quedarse estancadas en un sistema de trabajo arcaico, sin ningún tipo de control de las actividades que realizan. En el caso de las empresas con método de trabajo arcaico verían corregidos sus problemas implementando la norma ISO 9001, obteniendo sus productos y servicios un mayor grado de calidad. Las organizaciones de este tipo van a necesitar de la implementación de normas de gestión para no quedarse atrás de sus principales competidores.

En el caso de posibles riesgos que se pueden encontrar en la guía presentada son:

- Existe el riesgo de que algunas definiciones o lenguajes técnicos no sean comprensibles a la hora de interpretar la presente guía. Se ha tratado de introducir un lenguaje lo más coloquial y entendible posible.

- La guía ha seguido una explicación, de principio a fin, des del conocimiento de las normas hasta su certificación, es posible que extrayendo de contexto algunas de sus partes sea difícil interpretarla sin tener una visión de conjunto.

3.3 Identificación y análisis de soluciones posibles

En este proyecto se ha decidido como solución el realizar una guía aunque podrían haber opciones igual de eficaces como podrían ser:

-**Checklist:** La realización de un checklist consistiría en identificar paso a paso los objetivos que se deberían de alcanzar para conseguir implementar la norma e incluso certificarse en ella. Se iría marcando en dicha lista conforme se alcanzaran cada uno de los objetivos. El principal problema que podría surgir es que el checklist no sea lo suficientemente completo dejando aspectos de la norma sin incluir en el mismo, por tener algunos aspectos de las mismas diferentes interpretaciones.

-**Página web:** Crear una página web que dividiremos en diferentes secciones, donde se podrán encontrar las normas y el proceso de certificación, aportando información sobre estos puntos. En esta misma web podrá haber un foro, esto permitirá plantear y resolver dudas a los usuarios de un tema en concreto para se puedan ayudar entre ellos, donde se abrirán temas de debate. Se facilitará un correo electrónico atendido por el administrador, en el caso de que un usuario tenga una duda no resuelta. Se podría ganar dinero con ella publicitando a empresas. Para dar a conocer la web se podría mandar correos a empresas no certificadas informándoles del contenido de la misa, si esta web es muy buscada subirá puestos en el buscador de Google y será cada vez más probable que sea encontrada sin necesidad de publicitarla.

3.4 Solución propuesta

Como solución propuesta se presenta la guía, la cual nos va a permitir dar a conocer las tres normas de gestión a en empresas del sector de las tecnologías de la información y comunicación, con sus beneficios, y las principales pautas que se deberán de seguir si se quiere realizar una buena implementación de las normas. Posteriormente a la explicación de las normas, se expone la fase de implementación, explicando el proceso de auditoría interna, como continuación para aquellas empresas que deseen dar el paso de conseguir el certificado por medio de una empresa certificadora, se expondrá el procedimiento que deben seguir. Se podrá analizar cantidad de empresas certificadas en estas normas en los últimos años y por último, la experiencia real que han vivido dos empresas del sector TIC al realizar este proceso, y lo que les ha aportado.
Se ha elegido este formato para la solución debido a que visualmente introduce al lector en la temática, y no es un formato muy tedioso de leer. Con la guía podemos recopilar toda la información que se ha creído importante para conseguir la solución al problema que puedan tener las empresas o dudas que les puedan surgir.

3.5 Plan de trabajo

En este punto vamos a ver el calendario que se ha seguido para realizar este proyecto, donde se han realizado una planificación estableciendo objetivos cada semana para llegar a realizar el objetivo final, que es el presente trabajo. Se empezó a realizar este proyecto en Diciembre y han transcurrido ocho meses hasta llegar a la solución final.
La planificación que se ha seguido es la siguiente:

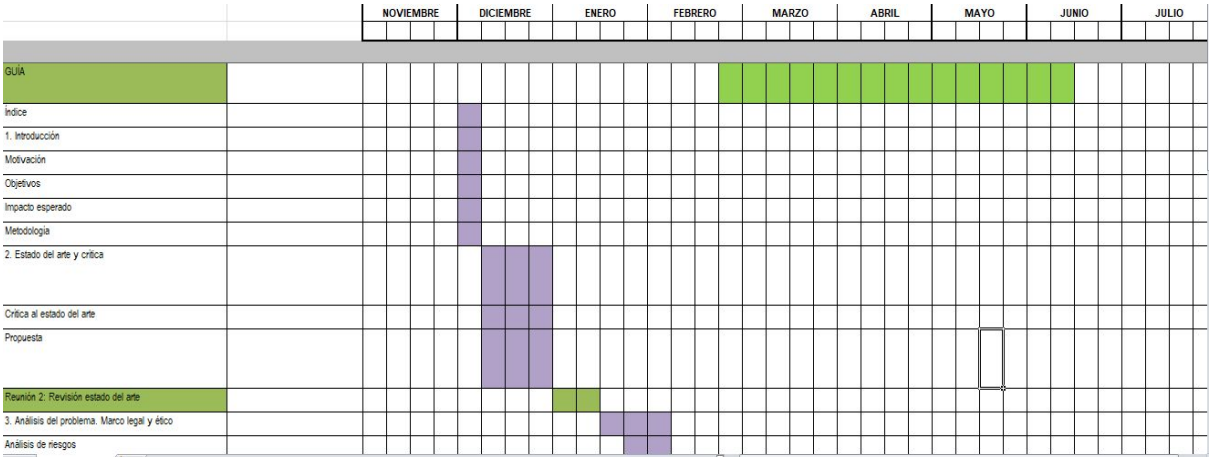


Imagen 3.5.1: Planificación 1.

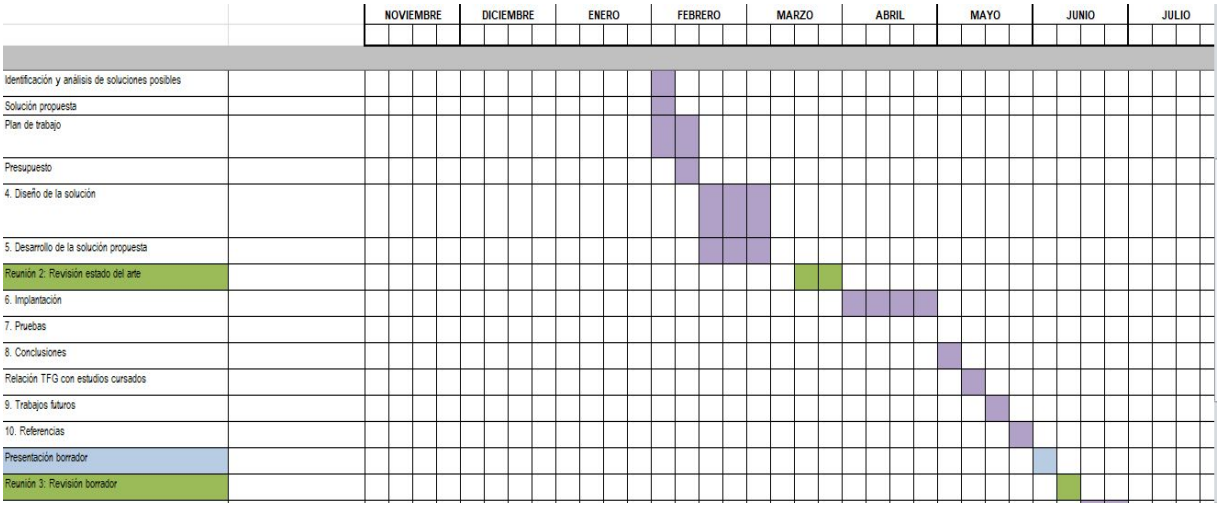
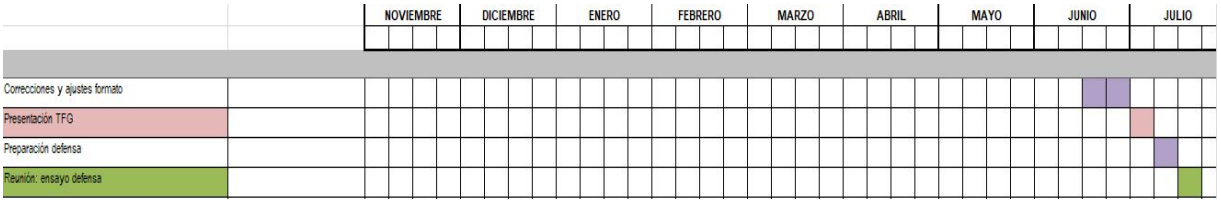


Imagen 3.5.2: Planificación 2.



I**magen 3.5.3**: Planificación 3.

3.6 Presupuesto

Para la realización del presupuesto se han tenido en cuenta jornadas laborales de 8 horas con un precio por hora de 15€ según el siguiente baremo:

- Trabajando 200 horas al mes.
- Teniendo en cuenta seguridad social, gasto de oficina…
- Desplazamientos.

Tiempo empleado para la elaboración de la guía han sido tres meses con un total de 600 horas trabajadas por un importe de 9000€.
Recursos empleados:

- Renting de ordenadores. (2 ordenadores a 29€ cada uno = 58 x 3 = 174€).
- Conexión a Internet. (70 x 3 = 210€).
- Impresión de la guía. (Impresión de 100 guías encuadernadas para su distribución a 7’5€ cada una = 7,5 x 100 = 750€).
- Compra de normas.(ISO 9001 = 124,09€, ISO 27001= 106,11€, ISO 20000-1 = 124,09€. Total = 354,29€)

Por lo tanto el importe total de nuestro trabajo sería de 10488,29€.
Se utilizarán libros basados en las normas y un ordenador para poder comprobar en diferentes webs la información necesaria, con su respectiva conexión wifi para poder navegar por internet. También se tendrán que hacer entrevistas a empresas del sector de las tecnologías de la información, y encuestas para comprobar qué información es

aquella que más falta pueda hacer para las empresas o en el caso de las encuestas que se envíen a empresas certificadas, los problemas que han encontrado y las ventajas, por lo tanto, habrá que tener en cuenta los desplazamientos que se hagan para el presupuesto final que hay que pasarle al cliente.
Una vez se tengan todos los gastos que se han realizado se le tendrá que pasar esta factura al cliente.

4. Diseño de la solución propuesta

El formato de solución por el que se ha optado es la realización de una guía : “Las normas de gestión de empresas y su aplicación a las empresas informáticas. La auditoría y la certificación de empresas”, en la cual se presentarán las ideas de una forma clara y bien estructurada, no tan tediosa para el lector, porque se pueden observar diferentes imágenes y visualmente es más ameno, que leer toda la información de un documento donde solo hay infinidad de líneas de texto.

En la guía se van a encontrar como apartados los siguientes puntos:

1. Introducción. Donde se va a presentar el trabajo y lo que nos va ayudar a comprender.
2. Normas de gestión. En este punto se va a comentar las normas de gestión respondiendo a preguntas como, ¿qué es una norma de gestión?, ¿qué es la ISO? Y una explicación de lo que es el ciclo PDCA. También encontraremos subapartados a lo largo de este punto donde se hablará de las tres normas de gestión ISO comentadas anteriormente, con una explicación de para qué sirven, sus beneficios si nos certificamos de ellas y las pautas para instaurar las normas.
3. Auditoría. Se contestan preguntas como, ¿qué es una auditoría? O ¿por qué es importante una auditoría?, también tendremos las pautas a seguir en una auditoría y el ciclo de vida de la misma.
4. Implementación de una norma. En este punto se habla de los pasos que se deben de seguir para la implementación de una norma y de la auditoría interna, explicada con más detalle en un subapartado de este punto.
5. Certificación. Se presenta información acerca del proceso de certificación, contestando a preguntas como ¿qué beneficios se obtienen al estar certificado?, ¿por qué adquirir el certificado? O ¿Cuánto cuesta certificarnos?, también se puede observar en qué consiste la auditoría de certificación, los tipos de certificados que se pueden encontrar y la cantidad de empresas que se certifican a lo largo de los últimos años de las tres normas. Por último, en este apartado se podrán ver las conclusiones a las que se ha llegado tras observar las respuestas de las encuestas.
6. Referencias. Sitios de donde se ha recopilado la información.
7. Anexo. Donde se añade información adicional a la expuesta en los anteriores puntos, que puede resultar de interés para el lector, como pueden ser un apartado donde encontramos las respuestas de las dos encuestas, que son las tecnologías de la información o la familia de las tres normas.

Esta es la información que se ha creído necesaria para completar la guía, ya que es lo que se estima que necesitaría conocer una empresa del sector no certificada que quiera obtener conocimientos de las normas, y aquello que les puede aportar el conseguir el certificado. Punto importante ha sido la tarea de investigación realizada para conseguir toda esta información, y las preguntas hechas a profesionales del sector para averiguar qué era aquello más conveniente que había que aportar al trabajo.

5. Desarrollo de la solución propuesta

En este punto se va a hablar de como se ha desarrollado la solución propuesta hasta llegar a la solución final.

La solución que se propuso en un primer momento fue la de realizar la guía, el problema que se tuvo es el no saber cómo plantear este trabajo y la selección de normas sobre las que se iba a trabajar. Tras buscar información acerca de las normas del sector de las tecnologías de la información y comunicación, se eligieron tres conocidas, pero que había que comprender para poder seleccionar la información más relevante para la organización y exponerla en la guía de un modo lo más comprensible posible.

Finalmente, en el tema de las normas de gestión, se acabó eligiendo como información importante una breve descripción de la norma, exponiendo cuál es su principal objetivo, los beneficios que va a aportar el estar implementado y certificado de la norma y las pautas para implementarlas.

Lo primero que se realizó en las normas de gestión fue introducirlas brevemente con su definición y con el ciclo PDCA. Por lo tanto, había que preguntarse acerca del proceso de implementación y certificación de las normas y cómo se conseguía una buena implementación y certificación de una norma Al buscar esta información también surgió respuesta al apartado de objetivos de cada norma, la cual hace referencia a los beneficios que se obtendrán al certificarse. Se investigó al respecto y se encontraron varias cosas a tener en cuenta para conseguir una correcta implementación mediante la ayuda de la auditoría interna. También se encontró el proceso que tiene que pasar una organización para conseguir el certificado, el cual es mediante la auditoría externa. Se llamaron a diferentes certificadoras para saber el precio de certificación en cada una de las tres normas que se ve plasmado también en la guía.

Para implementar las normas tenemos que tener en cuenta una serie de puntos, como pueden ser, explicar cualquier situación que pueda haber de dudas al personal de nuestra organización, explicando los beneficios que nos va a aportar el implementar la norma, teniendo un grupo de personas con conocimientos suficientes encargadas de realizar la implementación, pueden ser o bien de la organización, o bien de una empresa externa, y teniendo en cuenta que si queremos realizar una buena implementación, la organización deberá de realizar una auditoría interna por personas con suficiente conocimiento para hacerla, esta auditoría puede ser realizada por una empresa consultora o personal de la propia empresa, siempre realizándose con objetividad.

Una vez realizado esto, se deberá de decidir si la organización desea certificarse o no, en caso afirmativo se tendrá que realizar una auditoría externa contratando para conseguir el certificado a una organización certificadora, antes de ponerse en contacto con esta empresa, se puede solicitar una auditoría interna para comprobar si la organización cumple con los requisitos para conseguir el certificado. Si esta auditoría realizada anteriormente a la auditoría de la organización certificadora es buena, entonces se podrá seguir con la realización de la auditoría certificadora, pero si por el contrario obtenemos un resultado negativo, se deberá de reconsiderar algunos puntos. Estos puntos a considerar constaran en el informe realizado por el auditor, una vez

solucionados, la empresa debería de volver a pasar el mismo procedimiento de la auditoría interna, para comprobar que se ha solucionado todo como es debido y posteriormente pasar la auditoría certificadora.

El implementarse es un punto muy importante en todo este procedimiento y el que requiere un mayor tiempo. La encuesta realizada a S2 Grupo nos corrobora lo anteriormente dicho, si la empresa no está certificada por lo menos que esté implementada. El implementarse nos va a aportar grandes beneficios a la empresa, al igual que al certificarse va a dar mayor prestigio externo, ya que el hecho de estar certificado da a entender a los clientes potenciales y al resto de empresas que has hecho una buena implementación de la norma, y que por lo tanto cumples con los requisitos de esta y haces un buen uso de ella.

Hay que tener en cuenta que para mantener el certificado de estas normas, se tendrán que pasar por unas renovaciones, donde se realizará una auditoría de seguimiento a través de una empresa certificadora.

Todo esto está correctamente introducido y explicado en la solución final que es la guía.

6. Conclusiones

Para finalizar la memoria del presente trabajo, se mencionan las siguientes conclusiones:

- Al principio de la realización de la guía los conocimientos sobre las normas de gestión eran muy limitados, al ir investigando sobre los mismos uno se da cuenta del gran valor que potencialmente aportan a las organizaciones. Hay mucha información en Internet sobre estas normas, aunque utilizan muchos tecnicismos y muchas veces algunos procesos y definiciones son complicados de entender.

- La competitividad de las empresas en el sector de las tecnologías de la información es tan alta que seguir la guía que se ha planteado puede ayudar a la empresa a mantenerse en el mercado.

- Al poder hacer uso de la totalidad o parte de la información que aporta la presente guía, las empresas no familiarizadas con las normas pueden tener acceso a una gran cantidad de información.

- La presente guía se podrá ir modificando a medida que empresas que hagan uso de ella puedan identificar mejoras o incluso errores, siendo de este modo un proyecto siempre en continua mejora, aportando cada vez mayor valor y eficacia en cada actualización.

- Uno de los problemas encontrados durante la realización del presente trabajo, fue conseguir información de empresas no certificadas, a las que les pudiera interesar la guía, para conocer de primera mano si la orientación de esta era la correcta y que información se podría añadir.

- El problema que se encontró en el tema relacionado con las encuestas, es el saber si se iba a obtener respuesta de alguna organización o si las preguntas estaban correctamente planteadas. Se pidió una segunda opinión a una auditora para ver qué cambiar o qué preguntas añadir. Al final de todo el proceso se acabaron obteniendo dos encuestas respondidas de organizaciones de este sector.

- El proceso de certificación de las normas es largo y no es sencillo, se deben de seguir unas pautas y se necesita de la colaboración de los miembros de la organización. Una vez conseguida la certificación se ha de mantener buscando siempre nuevos objetivos de mejora.

- Este proyecto ha ayudado a ver las debilidades que existen a la hora de elaborar la redacción del mismo.

6.1 Relación TFG con estudios cursados

A lo largo de los cursos realizados en la ETSINF han habido cuatro asignaturas relacionadas con este trabajo final de grado. la cursada en segundo curso llamada Deontología y Profesionalismo (DYP), donde se introdujeron conceptos sobre la protección de datos y seguridad de la información. En tercero, está en la especialidad de sistemas de la información, la asignatura de Gestión de Servicios de sistemas de la información y tecnologías de la información (GSE), donde se expusieron trabajos en clase de algunas de las normas de gestión que existen, y durante la asignatura se explicó acerca de la seguridad de la información, la certificación y la auditoría. En cuarto curso en la especialidad anteriormente comentada, se cursaron dos asignaturas donde se puede encontrar información relacionada con este proyecto, en la asignatura de Calidad y Optimización (COP), en esta pasa algo similar al caso anterior donde los alumnos expusieron las normas de gestión, entre otras cosas. También encontramos la asignatura de cuarto curso Sistemas Integrados de información en las Organizaciones (SIO), en la cual se hablaron de las normas de gestión, del ciclo PDCA y de las tecnologías de la información.

Las competencias transversales más ligadas a este proyecto son:

- Innovación, creatividad y emprendimiento (Asignatura SIO): En este proyecto se ha buscado sobretodo la innovación y el emprendimiento en gran grado.
- Aplicación y pensamiento práctico (Asignatura COP): Se ha tenido que realizar un estudio acerca de normas de gestión aplicadas a empresas del sector de la tecnología de la información y comunicación por lo tanto, esta competencia transversal también ha sido importante en la realización del proyecto.
- Pensamiento crítico (Asignatura GSE): Esta competencia transversal también ha sido de gran importancia para saber entender, evaluar y analizar la información encontrada al realizar el trabajo de investigación, para luego plasmar las ideas en la guía.

Estas asignaturas han servido para darnos una base de información acerca de “la guía de las normas de gestión de empresas y su aplicación a empresas informáticas. La auditoría y certificación”, aunque cuando se busca mayor cantidad de información a la proporcionada por las asignaturas, uno se da cuenta de que este mundo es mucho más extenso, y complejo en algunos casos de entender, de lo que se creía.

7. Trabajos futuros

En este apartado se va a ver que se puede continuar trabajando de este proyecto, en este caso en la guía y cómo la podríamos mejorar.

Se podría realizar para este trabajo una página web con todos los contenidos de este proyecto para que cualquier empresa pueda entrar en ella y resolver cualquier duda que pueda tener relacionada con la guía, con información muy gráfica de las normas. Donde se podrían incluir con el paso del tiempo mayor cantidad de normas y más funcionalidades. Si una de las normas se actualiza también se podría informar de ello en esta web. Si se quisiera ganar algo de dinero mediante la web se podrían introducir anuncios de empresas. También se podría introducir un foro en esta web para discutir temas relacionados con la guía, para que los usuarios puedan resolverse dudas entre ellos y sea más dinámica.

Se podría realizar también una aplicación para dispositivos móviles, basada en la guía presentada, donde se podrán observar todas las definiciones relevantes y se distinguirá entre las diferentes normas de gestión, con posibilidad de hacer actualizaciones para ir añadiendo más contenido respecto al que se tiene inicialmente. Se podrán realizar críticas constructivas de la aplicación para mejorarla al correo proporcionado en la misma o incluso en la tienda de Android e IOS en el apartado de opiniones. La gran ventaja que tendría este trabajo es el poder tener toda esta información a mano en cuestión de segundos.

La ya comentada como solución alternativa checklist puede ser otra alternativa para elaborar en un futuro. En este caso el objetivo sería que la persona o personas encargadas de realizar la implementación de una norma de gestión, realizaran paso a paso aquellas tareas que nos marca la checklist y una vez finalizada cada tarea señalar la casilla en cuestión para dejar constancia de que se ha realizado. Esta solución nos va a permitir realizar todos los procesos de la implementación, sin dejar ninguno por hacer.

A este trabajo, por otra parte, se le podría añadir más información acerca de las normas ya tratadas e incluso añadir otras que puedan ser de interés del lector, teniendo siempre en cuenta, tener cuidado de no incluir términos muy técnicos para evitar que resulte tediosa su lectura.

8. Referencias

[1] Oltra Badenes, Raúl Francisco.*La norma ISO/IEC 20000. Finalidad y contenido*. Departamento de Organización de Empresas, Universitat Politècnica de València, 2017. [Fecha de consulta 17 de Abril 2019]. Disponible en: **http://hdl.handle.net/10251/84477**.

[2] Anduix Fuentes, J. (2015). Implementación de la norma UNE-ISO/IEC 27001 en una empresa de sector de servicios. Trabajo final de grado .Universitat politèctica de València. [Fecha de consulta 20 Abril 2019]. Disponible en: **http://hdl.handle.net/10251/54441**.

[3] Ugalde Canitrot, Arturo (2015). Gestión de calidad en epileptología. Valor de la certificación ISO 9000 en un laboratorio de monitorización vídeo-eeg. Tesis doctoral. Universidad Autónoma de Madrid. [Fecha de consulta 22 Abril 2019]. Disponible en: **https://www.educacion.es/teseo/mostrarRef.do?ref=1195566**.

[4] AJA QUIROGA, Lourdes. Gestión de información, gestión del conocimiento y gestión de la calidad en las organizaciones. *ACIMED*[en línea]. 2002, vol.10, n.5 [Fecha de consulta 24 Abril 2019], pp. 7-8. ISSN 1024-9435. Disponible en: **http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352002000500004&lng=es&nrm=iso**.

[5] Janett Yánez y Raiza Yánez. Auditorías, Mejora Continua y Normas ISO: factores clave para la evolución de las organizaciones. *Redalyc*[en línea]. 2012, vol.3, n.9, [Fecha de consulta 24 Abril 2019], pp. 83-92. ISSN 1856-8327. Disponible en: **http://servicio.bc.uc.edu.ve/ingenieria/revista/Inge-Industrial/volIII-n9/art7.pdf**

[6] Aenor, UNE-ISO/IEC 20000-1:2018, Tecnologías de la información. Gestión del servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio(SGS)[Fecha de consulta 3 Junio 2019]. Disponible en: **https://portal.aenormas.aenor.com/aenor/Suscripciones/Personal/pagina_per_buscador.asp**.

[7] Aenor, **UNE-EN ISO/IEC 27001:2017,** Tecnologías de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la Información. Requisitos. (IEC/ISO 27001:2013 incluyendo Cor:2014 y Cor 2:2015). [Fecha de consulta 5 Junio 2019]. Disponible en: **https://portal.aenormas.aenor.com/aenor/Suscripciones/Personal/pagina_per_buscador.asp**

[8] Aenor, UNE-EN ISO 9001:2015**,** Sistemas de gestión de la calidad. Requisitos (ISO 9001:2015)**.** [Fecha de consulta 5 Junio]. Disponible en: **https://portal.aenormas.aenor.com/aenor/Suscripciones/Personal/pagina_per_buscador.asp**

[9] Ladino A., Martha Isabel, Villa S., Paula Andrea, López E., Ana María, FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS. *Scientia Et*

Technica [en línea] 2011, XVII, páginas 334-339. (Abril-Sin mes) : [Fecha de consulta: 25 Abril de 2019]. ISSN 0122-170. Disponible en:**<http://www.redalyc.org/articulo.oa?id=84921327061>**

[10] Wouter Van den Berghe. Aplicación de las normas ISO 9000 a la enseñanza y formación. *Formación profesional Nº15 Revista Europea*. Páginas 21-30, ca. 2000.

[11] Bauset-Carbonell, María-Carmen y Rodenes-Adam, Manuel. Gestión de los servicios de tecnologías de la información: Modelos de aporte de valor basado en ITIL e ISO/IEC 20000. *El profesional de la información*, 2013, enero-febrero, v.22, n.1, páginas 54-61, ISSN:1386-6710.

[12] Santillana, Juan Ramón. *Auditoría interna*. Pearson Educación de México, SA de CV, 2011. [Fecha de consulta 23 Abril 2019]. ISBN 9786073220460. Disponible en: **http://www.ingebook.com/ib/NPcd/IB_Escritorio_Visualizar?cod_primaria=1000193&libro=6199**

9. Anexo

En este apartado se va a encontrar un glosario con las definiciones que se han creído que pueden ser más relevantes para el lector y la guía. Hay que tener en cuenta que la guía tendrá sus propias referencias y anexo.

9.1 Glosario

Mejora continua:
Actividad recurrente para mejorar el desempeño.

Eficacia:
Grado en el que se realizan las actividades planificadas y se logran los resultados planificados.

Manual de calidad:
Es un documento en el cual se encuentra la visión y misión de una empresa así como política de calidad y los objetivos que buscan que se cumpla esta política.

Sistema de gestión:
Conjunto de elementos de una organización que actúan o están interrelacionados para establecer objetivos, procesos y políticas para lograr dichos objetivos.

Legislación:
Conjunto o cuerpo de leyes por las cuales se regula un Estado, o materia determinada.

Objetivo:
Resultado a conseguir.

Organismo regulador:
Es una autoridad que consiste en asegurar la vida social y económica en un país.

Organización:
Grupos de personas o persona que tiene sus propias funciones con autoridad, relaciones y responsabilidad para lograr sus objetivos.

Proceso:
Conjunto de actividades que interactúan o interrelacionadas, que utilizan las entradas para proporcionar un resultado previsto.

Partes interesadas:
Organizaciones o personas que pueden afectar o verse afectadas por una actividad o decisión.

Política:
Dirección e intenciones de una organización como las expresa la alta directiva.

Contratar externamente:
Tener un acuerdo en el cual una organización externa realiza parte de un proceso o función en una organización.

Riesgo:
Efecto de incertidumbre.

Requisito:
Necesidad establecida, generalmente obligatoria o implícita.

Cliente:
Parte de una organización u organización que recibe uno o varios servicios.

Proveedor:
Empresa o persona que abastece de aquello que es necesario para un fin.

Seguridad de la información:
Preservación de la integridad, disponibilidad y confidencialidad de la información

Gestión de Calidad:
Procesos coordinados para controlar y dirigir una organización con respecto a la calidad.

Gestión de servicios:
Conjunto de procesos y capacidades para controlar y dirigir los recursos y actividades de la organización para el diseño, planificación, mejora y entrega de los servicios con el objetivo de entregar valor.

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

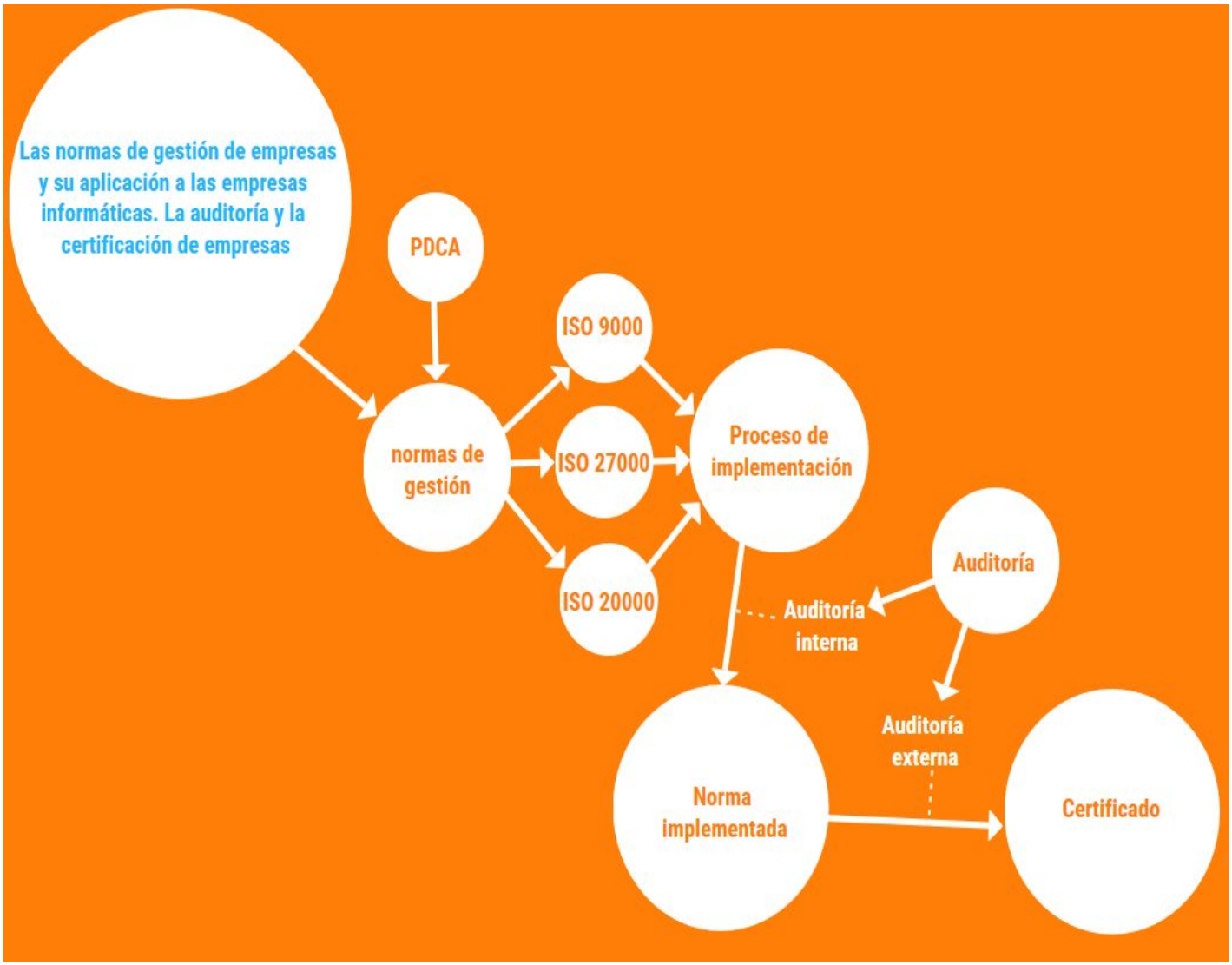
etsinf

Escola Tècnica Superior d'Enginyeria **Informàtica**

Guía de las normas de gestión de empresas y su aplicación a las empresas informáticas. Auditoría y certificación de empresas

Adrián Martínez Rochina

Universitat Politècnica de València


Las normas de gestión de empresas y su aplicación a las empresas informáticas. La auditoría y la certificación de empresas
PDCA
normas de gestión
ISO 9000
ISO 27000
ISO 20000
Proceso de implementación
Auditoría
Auditoría interna
Auditoría externa
Norma implementada
Certificado

ÍNDICE

1. ¿Qué pretendemos?

Esta guía nos va ayudar a entender las diferentes normas de gestión, también llamadas normas ISO, que podemos encontrar en empresas del sector de las tecnologías de la información y comunicaciones, identificando de qué nos va a servir estar certificados en las mismas, el proceso de certificación y los beneficios que la certificación puede aportar a la organización. Se tratará el tema de la auditoría, tanto externa como interna, y nos centraremos en las tres normas que se han considerado más importantes:

- La ISO 9000:2015. Sistemas de gestión de calidad.
- La ISO 20000:2018. Tecnologías de la información (TI). Gestión de los servicios.
- La ISO 27000:2019. Sistemas de gestión de la seguridad de la información.

Este documento pretende responder a aquellas dudas que como gerente, responsable de TI, etc. Se os planteen de cara a afrontar un proceso de implantación y certificación.

Al principio incluso la terminología es compleja, pero se espera que esta guía despeje las dudas que puedan tener.

2. NORMAS DE GESTIÓN

2.1 ¿Qué es la ISO?

ISO (Organización Internacional de Normalización) es la federación mundial de organismos internacionales de normalización. Se fundó para crear un conjunto de normas para la manufactura, las comunicaciones y el comercio.

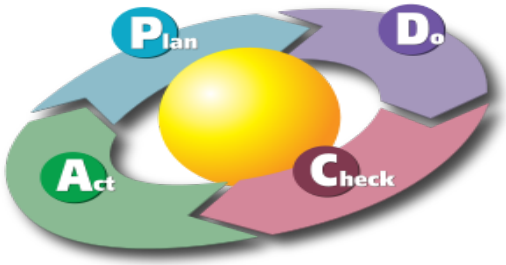
2.2 ¿Qué es una norma de gestión?

Son aquellas normas que nos van a ayudar a gestionar de una manera eficaz y eficiente la organización, esta gestión aportará beneficios en todos los niveles, como es la satisfacción de nuestros clientes y los conocimientos necesarios para que una empresa pueda tener éxito.

Mejorará la eficiencia de los procesos de la empresa y establecen un sistema de gestión de calidad reconocido, facilitando la comunicación, las negociaciones y comercios a nivel mundial.

2.2.1 PDCA

Las normas seguirán el ciclo **PDCA,** también es conocido como ciclo de Deming, describe las cuatro etapas esenciales que se deben de realizar si se quiere conseguir la mejora continua. Son cuatro etapas cíclicas, una vez finalizada la última etapa se deberá de volver a la primera para que se pueda volver a llevar a cabo el ciclo, así todas las actividades se vuelven a evaluar periódicamente para incorporar las nuevas mejoras o cambios en la organización.



Las cuatro etapas que lo componen son:

1. **Planificar (Plan)**: Ver una oportunidad de mejora y planificar los cambios para que se produzca esta mejora. Herramientas que podemos encontrar para la planificación son por ejemplo el diagrama de Gantt, Análisis Modal de Fallos y Efectos(AMFE),DAFO, CAME, etc.
2. **Hacer (Do)**: Se realizan los cambios para implantar la mejora propuesta y se prueban.
3. **Controlar o verificar (Check)**: Cuando ya se ha implantado la mejora, tendremos que realizar una revisión para comprobar esta implantación y analizar los

resultados. Si la mejora no cumple las expectativas, se deberán de realizar los cambios necesarios para ajustarla a los objetivos esperados. Ejemplos de herramientas de evaluación que podemos encontrar son por ejemplo, una check list, diagrama de pareto, cuadro de mando, etc.

4. **Actuar (Act)**: Realizar acciones basadas en lo aprendido en la etapa de control. Si encontramos datos satisfactorios se implantará la mejora, en cambio si estos datos no son satisfactorios, habrá que que volver a empezar el ciclo con otro plan. Una vez realizado este paso y como se ha comentado con anterioridad se deberá de volver al primer paso.

2.3 ISO 9000:2015 Sistemas de Gestión de la Calidad

Las ISO 9000 son el conjunto de normas que establecen las indicaciones para conseguir un producto o servicio final de calidad y un sistema de gestión de calidad eficiente y correcto.

Un sistema de gestión de calidad se encarga de gestionar los recursos y procesos que se necesitan para proporcionar valor y conseguir los resultados para las parte interesadas, entender actividades en las que la organización identifica sus objetivos y determina los recursos y procesos necesarios para lograrlos, posibilita a la dirección optimizar el uso de recursos y proporciona medios para identificar la previsión de las consecuencias en la provisión de servicios y productos. Un ejemplo de sistema de gestión de calidad es el de Coca-Cola la cual busca que la bebida cumpla con las expectativas del consumidor, procura optimizar los procesos logísticos e industriales y garantizan la implementación de las políticas de calidad, donde se proporcionan los recursos necesarios para alcanzar los objetivos.

Esta familia de normas es una de las más importantes que podemos encontrar hoy en día, cualquier tipo de empresa se puede certificar con el certificado ISO 9001, ya que se adapta bien al servicio proporcionado o al producto final que se quiera vender, por lo que es una serie de normas bastante flexible.

Cuando una organización consigue adoptar la ISO 9004 alcanza el más alto rango en esta serie de normas y esto ayuda a mejorar el sistema de gestión de calidad de la organización.

2.3.1 Objetivos de la familia ISO 9000

El fin que persigue esta serie de normas consiste en que las empresas consigan conocimientos de lo que es un sistema de gestión de calidad y de su implantación. El objetivo principal que tiene esta familia de normas es dar a conocer y dominar los aspectos de la gestión de la calidad.

Los beneficios que encontramos son:

- Ventaja frente a nuestros competidores del sector.
- Asegurar el cumplimiento de los objetivos.
- Reducción de costes.
- Conseguir capacidad de liderazgo.
- Satisfacción del cliente.
- Mejora continúa.
- Aumento de la productividad.
- Relaciones con proveedores.
- Personal comprometido y con mayor confianza en la organización.
- Efectividad en la toma de decisiones.

2.3.2 ¿Cómo instaurar un sistema de gestión de calidad?

Se deberán de seguir una serie de etapas para poder instaurar un sistema de gestión de calidad, se podrán realizar modificaciones en el futuro para mantener este sistema al día:

- Información. Tener conocimientos de la norma para poder implementarla, consultando, por ejemplo, el documento publicado por Aenor sobre el contenido de dicha norma.
- Planificación. Se realiza un plan para la implementación de la norma de gestión ISO 9001 actualmente en vigor.

- Desarrollo. Habrá que realizar una documentación del sistema de gestión de calidad, incluyendo los procedimientos, manual de calidad, mapa de procesos y política de calidad. Aquí se desarrollará el manual de calidad y aquellos procesos que sean necesarios para el sistema.
- Capacitación. Los empleados recibirán formación acerca del contenido de la norma, elaboración de procedimientos, creación de pautas de registro, instrucciones de funcionamiento por parte de consultores externos.
- Auditorías internas. Deberá de pasar una auditoría interna para completar la instauración. La auditoría interna está explicada en el punto 4.1 con más detalle.

2.4 ISO 20000:2018 Gestión de los servicios de las tecnologías de la información

Es un conjunto de normas internacional basada en la gestión de servicios de tecnologías de la información. Estas normas nos describen un conjunto de procesos de gestión diseñados para facilitar los servicios TI,[1] ya que cada vez nos encontramos que estos servicios son más complejos, y nos proporcionará una metodología que le ayudará a gestionar su gestión de servicios de TI (ITSM) y con ella se muestra que nuestra empresa sigue buenas prácticas.

La ISO 20000 está basada en ITIL(es una colección de libros que trata sobre la gestión de servicios de las tecnologías de la información), la gran diferencia es que ITIL certifica a las personas y la norma es para las empresas.

Esta serie de normas es muy importante, debido a que una organización depende de su TI para llegar a alcanzar los objetivos que se propone. Esta norma describe diferentes procesos que se agrupan en 6 bloques:

- Portfolio de servicios
- Relación y acuerdo
- Oferta y demanda
- Ejecución y resolución
- Diseño, transición y construcción de servicios.
- Aseguramiento de servicios.

los procesos que corresponden a cada bloque se pueden ver en apartado 7.4 del anexo y tienen que aplicarse a los servicios que nos presta el departamento de tecnologías de la información, con el objetivo de gestionar y mejorar la calidad de estos servicios .Las empresas pueden certificarse de la norma de gestión ISO 20000-1.

[1] TI: Tecnología de la información

2.4.1 Objetivos de la familia ISO 20000

Los objetivos que tienen la familia ISO 20000 serán los siguientes:

- Mejorar la imagen y credibilidad de la organización.
- Hacer a nuestra empresa más productiva.
- Gran satisfacción de nuestros clientes y clientes potenciales.
- Reducción del coste.
- Mayor facilidad de adaptación.
- Solución de problemas basados en nuestro sistema de gestión de servicios de TI.
- Mejora continua.
- Ventajas frente a nuestros competidores.

2.4.2 ¿Cómo instaurar un sistema de gestión de servicios de TI?

Si queremos certificarnos de esta serie de normas, a parte de tener la documentación oportuna también, se tendrá que informar a cerca de las actividades que realiza la organización día a día. Otros pasos que se deberán de tener en cuenta si se desea implantar estas normas son:

- Identificar objetivos y beneficios esperados.
- Evaluar nivel de madurez de la empresa.
- Definir el alcance considerando los objetivos, política y beneficios.
- Asignar responsabilidades y recursos al Sistema de gestión y los procesos.
- Diseñar procesos.
- Gestionar los Sistemas de Gestión.
- Auditoría interna: Nos ayudará a encontrar posibles problemas y/o debilidades de nuestra organización, si no se realizara la auditoría podrían permanecer, y verificar sus procesos de ITSM.

2.5 ISO 27000:2019 Gestión de la Seguridad de la Información

La familia de normas ISO 27000 es un conjunto de estándares, que nos va a ayudar a operar o implementar un sistema de gestión de la seguridad de la información, para cualquier tipo de organización ya sea grande o pequeña. Las organizaciones pueden usar esta familia de normas para preparar una evaluación a su sistema de gestión de la seguridad de la información, y comprobar la protección de la información. Es una serie de normas considerada muy importante debido a que hoy en día la información es esencial para cualquier organización, por lo tanto, esta información deberá de estar protegida correctamente y no debe de salir a la luz sin ningún tipo de permiso. De esta familia de normas nos podremos certificar de la ISO 27001.

2.5.1 Objetivos de la familia ISO 27000

El principal objetivo que tiene la norma ISO 27000 es el de definir requisitos para un SGSI[2], que garanticen la selección de controles de seguridad adecuados y proporcionales para proteger la información. Por lo tanto, podemos decir que el objetivo que tiene esta serie de normas es la de proporcionarnos:

- Ayuda en la estructuración de la gestión de la seguridad de la información para la dirección.
- Buen uso de la seguridad de la información.
- Apoyo al proceso de operar, mantener, implementar y especificar un sistema de gestión de la seguridad de la información.
- Aumentar la confianza de las partes interesadas.
- Mejor gestión económica en la seguridad de la información.
- Disponer una base ideal y un lenguaje común para la seguridad de la información.

[2] SGSI: Sistema de gestión de la seguridad de la información. Es una perspectiva sistemática para operar, implementar, establecer, mejorar y monitorizar la seguridad de la información de una empresa para alcanzar los objetivos.

2.5.2 ¿Cómo instaurar un sistema de gestión de seguridad de la información?

Los pasos que deberemos de seguir para instaurar un SGSI será el siguiente por este orden:

1. Redactar una política de SGSI.
2. Asignar las responsabilidades de seguridad.
3. Se debe de concienciar a todos los empleados de todo aquello relacionado con la seguridad de la información y ayudarlos a entender las nuevas políticas y procedimientos.
4. Plan de tratamiento de riesgos. Hay que registrar todas las incidencias que ocurran en este proceso y su impacto, por lo que hay que realizar controles de detección de estos riesgos y actuar ante ellos.
5. El SGSI que queremos implantar tendrá que mantener en las características básicas de nuestra organización, no se debe perder aquello por lo que se creó la empresa.
6. Guardar los registros. Hay que cuidar como es debido la información ya que se deben de cumplir las propiedades de: integridad, confidencialidad y disponibilidad.
7. Protección de los datos.
8. Derechos de propiedad intelectual. Hay que tener todas las licencias en orden.
9. Comprobar que los resultados del SGSI son los esperados.
10. Se realizará una auditoría interna.

3. Auditoría

3.1 ¿Qué es una auditoría?

Una auditoría es un proceso:

- **Sistemático:** La auditoría se realiza de manera ordenada, de acuerdo a un método establecido.
- **Independiente:** La auditoría debe ser llevada a cabo por personas que aseguren la objetividad e imparcialidad de la misma.
- **Documentado:** El proceso de auditoría se recoge en un procedimiento escrito y sus resultados deben registrarse.

La persona que realiza la auditoría se le conoce como auditor y su función consiste en verificar y comprobar que los datos de la empresa a la que realiza la auditoría corresponden con los datos de las actividades que se han ido realizando dentro de la organización. Una vez finalice la auditoría el auditor redactará un informe con todos los datos obtenidos de la organización.

3.2 ¿Por qué es importante la auditoría en una empresa?

Hay personas que dependen directamente del trabajo que se realiza dentro de una organización por lo tanto, se debe de tener un control de que aquello que se realiza es lo correcto. La organización tendrá que dar a ver qué hace un buen uso de los recursos utilizados y tendrá que mantener en orden todas las regulaciones legales.

Si mediante la auditoría la empresa da a ver que tiene todo correctamente establecido, esto va a ayudar a que los inversores y clientes que tenemos tengan mayor confianza en lo que hacemos y puede llegar a atraer a nuevos. La auditoría puede ayudar a las organizaciones a optimizar sus operaciones y ahorrar importantes cantidades en los costos que se tenga.

Cuando no se cumplen los resultados esperados por la empresa en cualquier sector ya sea en quejas, más gastos de los esperados o imcumpliento de proyectos, entre otras cosas, es necesario realizar una auditoría. Existen dos tipos de auditorías de las que se van a hablar, en el apartado de implementación de la auditoría interna y en el apartado de certificación de la auditoría externa.

3.3 ¿Qué pautas debe de seguir una auditoría?

Para la realización de una buena auditoría hay que tener en cuenta las siguientes pautas:

- **Programación:** La frecuencia con la que se realizarán las auditorías se establecerá en función del estado e importancia de los procesos y las áreas a auditar.
- **Auditores:** Los auditores deben de asegurar la objetividad e imparcialidad de la auditoría. Deben de tener los conocimientos necesarios para su realización.
- **Resultados:** Se deben de registrar y transmitir al personal que tenga responsabilidad en el área auditada para que tomen acciones.
- **Acciones correctivas:** Cuando en la auditoría aparecen no conformidades, el personal responsable de las áreas auditadas propondrá e implementará acciones correctivas lo antes posible.
- **Seguimiento de la auditoría:** Las actividades de seguimiento deben de incluir la verificación de las acciones tomadas y el informe de los resultados de la verificación.

3.4 ¿Cuál es el ciclo de vida de una auditoría?

El ciclo básico realizado en una auditoría corresponde con lo siguiente:

- **Toma de contacto:** Conocer la organización que se va a auditar por parte del auditor.

- **Alcance:** Reúne aquello que se va a necesitar para cumplir con los objetivos que nos proponemos al realizar el proyecto, lo que nos indicará cómo actuar para alcanzar los objetivos.
- **Documentación y actividades:** Se hará una revisión de la documentación y se empezarán a preparar las actividades a realizar, es el momento donde se define el plan de auditoría, se prepara la inspección y los documentos correspondientes, es posible que personas de la organización tengan que colaborar.
- **Desarrollo del plan de la auditoría:** Plan donde se detallan todos los procesos por los que se han pasado y los resultados obtenidos para facilitar la información a un auditor externo por ejemplo. Donde se explican los objetivos de la auditoría, su alcance y todo acerca de la evidencia documentada de la auditoría. Se deberán de tener en cuenta los dos puntos anteriores.
- **Auditoría:** Este es el punto donde el auditor recogerá todos los datos obtenidos durante este proceso.
- **Informe de la auditoría y resultados:** Cuando se han detallado todos los procesos y se han finalizado las acciones del plan de auditoría, se redactará un informe donde deberá de aparecer toda la documentación de la auditoría correctamente comentada y a que punto se ha llegado después de realizar todo este proceso. Se presentarán los resultados obtenidos tras haber hecho todo el ciclo.

4. Implementación de una norma

La implementación de una norma de la Organización Internacional de Normalización no proporciona el certificado de la misma. Para tener una buena implementación de una norma se hará uso de la auditoría interna mientras que si queremos certificarnos posteriormente a la fase de implementación y al haber pasado la auditoría interna, se deberá de pasar una auditoría de certificación (de la cual se hablará en el punto 5.3).

La implementación es un primer paso hacia la certificación. Para implementar una norma ISO se deberán de tener en cuenta los siguientes puntos:

- Informarse acerca de la norma que se quiera implantar e informar acerca de esta al resto de la organización, donde explicaremos en que nos va a beneficiar la implementación de la norma dentro de la empresa, los objetivos que hay que tener en cuenta para implantarla, el tiempo que nos va a llevar a cabo ponerla en funcionamiento y cuánto nos va a costar. Una de las partes que nos va a ayudar es la implicación de todos los empleados, a los cuales se les deberán de aclarar cualquier duda que pueda surgir acerca del proyecto.
- Se necesitará un grupo de personas o persona encargada de realizar el trabajo específico de la implementación, donde se deberá de elegir si se va a querer certificar, en ese caso elegir qué empresa externa será la encargada Habrá que evaluar, analizar y medir los recursos que se van a necesitar para este proceso y el diagnóstico de las necesidades de capacitación.
- La persona o personas encargadas tendrán que realizar un sistema de gestión para obtener mejores resultados en los procesos internos, explicando las actividades que se llevan a cabo en la organización, como son los procesos que intervienen y la visión y misión de la organización junto con la política de calidad y sus objetivos.
- Poner en funcionamiento el sistema de gestión para lograr los objetivos marcados.
- El último apartado de la implementación es la auditoría interna de la que hablaremos con más detalle en el punto siguiente.

Cabe destacar que aunque la empresa no se certifique el simple hecho de realizar una correcta implementación de la norma es un paso muy importante para buscar la mejora de la organización.

4.1 Auditoría interna

Es aquella que vamos a realizar en la fase final cuando se quiera implementar una norma de la Organización Internacional de Normalización en nuestra empresa. La realizará o bien alguien de la organización que tenga los conocimientos técnicos suficientes como para realizarla o bien se deberá de subcontratar una empresa consultora, el auditor deberá de

ser completamente objetivo. La empresa deberá de facilitarle la información que el auditor precise para realizar la auditoría y pueda realizar un trabajo de investigación minucioso, el trabajo tiene que ser profesional y aunque pertenezca a la propia organización deberá de ser totalmente imparcial. Para la realización de la implementación no es lo único para lo que nos va a servir este tipo de auditoría ya que nos va a ayudar a ver el estado de nuestra organización, lo que permitirá darse cuenta de posibles riesgos de no superar la auditoría externa si se quisiera conseguir el certificado en nuestra empresa y resolver estos posibles problemas lo antes posible. Conforme la organización vaya creciendo la realización de una auditoría interna va cobrando más fuerza. La auditoría interna es una prueba final para comprobar cómo se ha llevado a cabo la implementación y se comprueba el cumplimiento de la norma.

La auditoría interna nos va a ayudar en gran medida a aumentar la posibilidad de que la empresa pueda lograr sus objetivos.

5. Certificación

5.1 ¿Por qué adquirir el certificado?

Si lo que se busca es dar una buena salida a tú empresa, la certificación es un buen método para lograrlo, ya que se mejora la eficiencia de la organización al igual que su rentabilidad, mientras que se va a tener un mayor reconocimiento a nivel internacional y el certificarse también ayudará a ser más competitivo frente a nuestros principales competidores.

Los certificados ISO nos van a garantizar que se cumple una determinada normativa ISO y todos los estándares de esta normativa están implementados como marca la norma en cuestión.

5.2 ¿Qué beneficios se obtienen al estar certificados?

El estar certificado provocará a la empresa tener una serie de beneficios que son los siguientes:

- Mejorar la imagen de cara a los clientes actuales y clientes potenciales.
- La productividad irá en aumento ya que siempre se buscará la mejora continua.
- Mayor confianza en el entorno de la empresa como son los proveedores, administraciones públicas y clientes.
- Cuando una compañía obtiene un certificado o certificados pertinentes, se conoce que es un empresa fiable.
- Menor tiempo a la hora de realizar una toma de decisiones.
- Se incrementa el volumen del negocio al igual que se produce un incremento del prestigio al estar certificado de una normativa ISO.

5.3 Auditoría de certificación

Es aquella que nos va a ayudar a conseguir el certificado, en este caso el auditor pertenece a una organización certificadora(Aenor, SGS España, Applus certification,etc.), por lo que viene de una empresa externa y no tiene relación con la empresa que va auditar. La

organización certificadora ha de ser acreditada por organismos de acreditación para ofrecer los servicios de auditoría y certificación.

Es el último paso hacia el certificado de una norma. Los datos de la organización tienen que ser los mismos que reflejan los documentos que ha extraído el auditor.

La organización puede contratar a una empresa consultora, para la realización de una auditoría interna, que verifique que está todo correctamente implementado y en orden para que pueda pasar la auditoría de la organización certificadora, y así conseguir el certificado. En caso de no tenerlo todo como es debido nos informarán de qué mejorar, para así poder solucionar los errores y pasar posteriormente la auditoría y conseguir el certificado.

5.4 Tipos de certificados

Encontramos diferentes normas dentro de las diferentes familias de ISO pero no de todas estas normas podemos adquirir un certificado. A continuación se van a nombrar algunas de las diferentes normas de las que podemos conseguir certificarnos y en qué campos se encuentran:

1. Certificados ISO de Gestión de la Calidad:

   - ISO 9001:2015. Sistemas de gestión de la calidad.

   - ISO 20000-1:2018. Tecnologías de la información (TI). Gestión de los servicios.

2. Certificados ISO de Gestión Ambiental

   -ISO 14001:2015. Sistemas de gestión ambiental.

3. Certificados ISO de Riesgos y Seguridad

   - La ISO 27001:2019. Sistemas de gestión de la seguridad de la información

   -ISO 22301:2015. Protección y seguridad de los ciudadanos. Sistema de gestión de la Continuidad del Negocio.

   -ISO 39001:2013. Sistema de gestión de la seguridad vial.

   -ISO 45001:2018. Sistema de gestión de la seguridad y salud en el trabajo.

5.5 ¿Quién acredita a las empresas certificadoras?

La Entidad Nacional de Acreditación (ENAC) establece los requisitos generales que deben de cumplir las empresas de certificación de sistemas de gestión, estos requisitos están relacionados en la norma ISO/IEC 17021-1 y en el documento CGA-ENAC-CSG y de obligado cumplimiento si una organización certificadora quiere conseguir la acreditación.

5.6 ¿Cuánto cuesta certificarnos?

El coste de certificación es un poco variable ya que hay que tener en cuenta diferentes factores a la hora de lograr el certificado:

- El primer paso y más importante es la implementación donde se tendrá que conocer ante todo de aquello de lo que nos queremos certificar. Deberemos de pagar un curso para los empleados y aquellas personas que vayan a estar en el proceso de certificación, donde el precio variará dependiendo de los conocimientos que tenga cada miembro y dependiendo del curso en cuestión, si existen empleados que no tenían conocimientos anteriores lo más probable es que este curso no sea suficiente, en este caso se necesitará de ayuda de consultores externos a la empresa para ayudar en este proceso de implementación.
- A los empleados que vayan a formar parte del equipo que busque la certificación, se le deberá de contribuir en su salario con este esfuerzo extra que se está realizando, aunque también se pueden contratar empleados de una empresa externa para la realización de este trabajo.
- Por último tendremos el coste de las auditorías que comprobarán que se sigue cumpliendo en la organización las normas o norma ISO de la que nos hemos certificado. Se realizará un seguimiento de durante un período como mínimo de tres años donde se realizará una recertificación con un coste menor.

Los costes que se pueden encontrar para certificarnos varía dependiendo de la certificadora. Aquí tenemos algunos ejemplos tomando como base una PYME (pequeña y mediana empresa), de hasta 15 trabajadores, de modo que los precios tuvieran una misma referencia para poder compararlos:

Bureau veritas:

- ISO 9001: 1125€ el primer año y los dos años posteriores 750€ cada uno, haciendo un precio total en tres años de 2625€.
- ISO 27001: 1500€ el primer año y los dos años posteriores 850€ cada uno, haciendo un precio total en tres años de 3200€.
- ISO 20000-1: 1500€ el primer año y los dos años posteriores 800€ cada uno, haciendo un precio total en tres años de 3100€.

Applus:

- ISO 9001: 1500€ el primer año y los dos años posteriores 750€ cada uno, haciendo un precio total en tres años de 3000€.
- ISO 27001: 1000€ el primer año y los dos años posteriores 500€ cada uno, haciendo un precio total en tres años de 2000€.
- ISO 20000-1: 525€ el primer año y los dos años posteriores 300€ cada uno, haciendo un precio total en tres años de 1125€.

Sgs:

- ISO 9001: 2250€ el primer año y los dos años posteriores 1100€ cada uno, haciendo un precio total en tres años de 4450€.
- ISO 27001: 4200€ el primer año y los dos años posteriores 3600€ cada uno, haciendo un precio total en tres años de 11400€.
- ISO 20000-1: 4200€ el primer año y los dos años posteriores 3600€ cada uno, haciendo un precio total en tres años de 11400€.

Hay que tener en cuenta que el precio de las dos primeras va a en función de que la auditoría externa dura dos días mientras que en el caso de Sgs la auditoría de la ISO 9001 dura dos días y medio y la 27001 y 20000-1 dura tres días y medio.

El ciclo inicial de certificación suele ser de tres años siendo la cantidad de tiempo empleado en las auditoría de seguimiento (las auditorías del segundo y tercer año) un tercio del tiempo empleado en la auditoría inicial.

El precio lo va a marcar la durabilidad de la auditoría externa y esta duración irá en función de la complejidad de la organización y de la cantidad de empleados que tenga. Estas indicaciones las realiza ENAC (Entidad Nacional de Acreditación). La tabla siguiente nos indica los días a emplear en la auditoría según el número de trabajadores y su complejidad:

Número efectivo de empleados	Duración auditoría Etapa1 + Etapa 2 (Auditor · día)				Número efectivo de empleados	Duración auditoría Etapa 1 + Etapa 2 (Auditor · día)			
	Alto	Medio	Bajo	Limitado		Alto	Medio	Bajo	Limitado
1-5	3	2.5	2.5	2.5	626-875	17	13	10	6.5
6-10	3.5	3	3	3	876-1175	19	15	11	7
11-15	4.5	3.5	3	3	1176-1550	20	16	12	7.5
16-25	5.5	4.5	3.5	3	1551-2025	21	17	12	8
26-45	7	5.5	4	3	2026-2675	23	18	13	8.5
46-65	8	6	4.5	3.5	2676-3450	25	19	14	9
66-85	9	7	5	3.5	3451-4350	27	20	15	10
86-125	11	8	5.5	4	4351-5450	28	21	16	11
126-175	12	9	6	4.5	5451-6800	30	23	17	12
176-275	13	10	7	5	6801-8500	32	25	19	13
276-425	15	11	8	5.5	8501-10700	34	27	20	14
426-625	16	12	9	6	>10700	Seguir la progresión			

Figura 5.6.1: Días auditoría certificadora

La etapa 1 equivale al proceso de planificación de la auditoría, se visita la organización, confirmar el plan de auditoría. Al finalizar la auditoría inicial en la etapa 2 el auditor documentará los procesos que han sido auditados. Estas etapas se producen durante la primera certificación.

En este gráfico se puede observar como se define la complejidad de una organización:

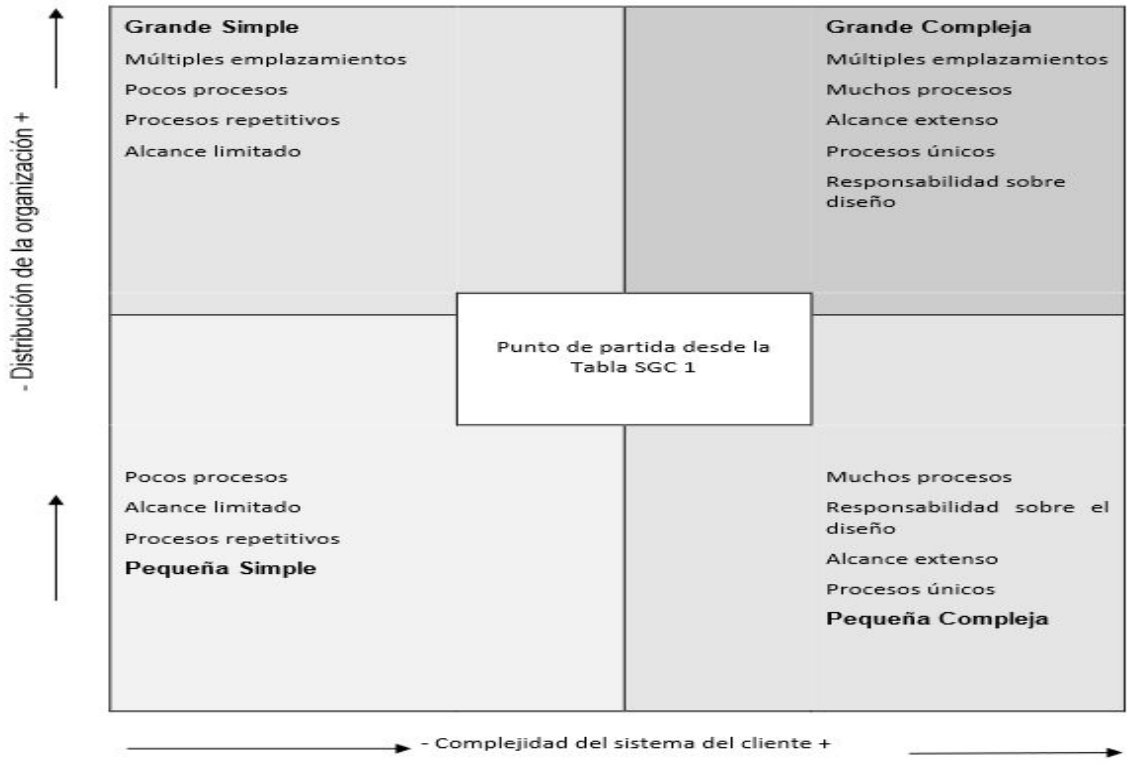


Figura 5.6.2: Grado de complejidad

Arriba a la derecha será el mayor grado de complejidad mientras que abajo a la izquierda obtendremos el menor.

5.7 ¿Es necesario certificarnos?

No es ni obligatorio ni necesario certificarnos pero el hacerlo sí que nos va a aportar una serie de ventajas anteriormente comentadas. Hay que tener en cuenta que a la hora de conseguir un certificado se necesita pasar por un proceso de implementación, con sus correspondientes auditorías internas y posteriormente contactando con la organización certificadora para realizar la auditoría externa, esta organización comprobará que la empresa cumple con las condiciones necesarias para lograr el certificado.

Es un proceso que puede ser largo para la organización, desde que se empieza con el proceso de implantación hasta que se consigue el certificado, pero el conseguirlo le puede

merecer la pena a la empresa. Lo que sí que es realmente recomendable es que la organización realice la implementación de la normativa que desee.

5.8 ¿Se certifican las empresas de la ISO 9001?

Tener un sistema de gestión de calidad es bastante importante en una organización aunque podemos ver en las imágenes que tenemos a continuación como con el paso del tiempo se han ido certificando de esta normativa menos empresas en Europa y en España. Lo más probable es que las empresas ya tengan este certificado y lo único que tienen que hacer es renovarlo con el paso del tiempo, también existe la posibilidad que dejen de renovarlo porque supone un coste para la empresa que seguramente no quieran pagar.

ISO 9001 - Quality M

Year	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
TOTAL	**980322**	**1063751**	**1076525**	**1009845**	**1017279**	**1022877**	**1036321**	**1034180**	**1105937**	**1056855**
Africa	8534	8435	7667	8164	9674	9816	10143	12154	13378	11210
Central and South America	37458	35549	49260	51685	51459	52466	50165	49509	52094	45541
North America	47896	41947	36632	37530	38586	48579	41459	46938	44252	38218
Europe	455303	500286	530039	459367	469739	458814	453628	439477	451415	387836
East Asia and Pacific	366491	408498	396492	402453	396398	387543	414801	422519	480445	513742
Central and South Asia	44171	44432	37596	33577	32373	44847	44790	40822	41370	39887
Middle East	20469	24604	18839	17069	19050	20812	21335	22761	22983	20421

ISO 9001 - Europe

Year	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Country										
Spain	68730	59576	59854	53057	59418	42644	35995	32730	34438	31984

A continuación se puede observar la cantidad de certificaciones de esta normativa en las empresas TICS, en este caso sí que podemos observar a lo largo de los años una subida importante, cosa que no pasa en los casos anteriores:

ISO 9001 - Certificates by Industrial Sector

EA* Code Nos.	ISO 9001 BY INDUSTRIAL SECTOR	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
33	Information technology	12505	21410	18998	20467	24690	27229	28995	29162	35268	33664

5.9 ¿Se certifican las empresas de la ISO 2000-1?

El caso contrario pasa en la normativa de gestión de los servicios de las tecnologías de la información, como se puede ver, se produce un incremento de los certificados a lo largo de los años en Europa pero en España sucede el caso contrario ya no se certifican tantas empresas, lo más probable es que las empresas ya tengan esta normativa y lo único que tengan que hacer para mantenerla es renovarla cada cierto período, pasa exactamente lo mismo que que se ha comentado en el punto anterior:

ISO/IEC 20000-1:2011 - Information Technology - Service Management

Overview

Year	2015	2016	2017
TOTAL	**2778**	**4537**	**5005**
Africa	25	38	46
Central / South America	88	119	144
North America	254	276	367
Europe	1.120	1.320	1.378
East Asia and Pacific	758	2.227	2.448
Central and South Asia	434	447	494
Middle East	99	110	128

ISO/IEC 20000-1:2011 - Europe

Year	2015	2016	2017
Country			
Spain	231	215	197

Mientras que en las empresas de las tecnologías de la información encontramos que se produce un incremento conforme pasan los años como se puede observar:

ISO 20000-1 - Certificates by Industrial Sector

EA* Code Nos.	ISO 20000-1 BY INDUSTRIAL SECTOR	2015	2016	2017
33	Information technology	735	876	1358

5.10 ¿Se certifican las empresas de la ISO 27001?

Cada vez más empresas buscan adquirir el certificado en esta normativa de gestión de la seguridad de la información, ya que buscan proteger sus datos y que no salgan al exterior sin permiso de la propia organización, aquí se puede ver cómo se están incrementando las empresas que se certifican de esta norma año a año, tanto en Europa y el resto de continentes, como en España:

ISO/IEC 27001

Year	2012	2013	2014	2015	2016	2017
TOTAL	**19620**	**21604**	**23005**	**27536**	**33290**	**39501**
Africa	64	99	79	129	224	301
Central / South America	203	272	273	347	564	620
North America	552	712	814	1445	1469	2108
Europe	6379	7952	8663	10446	12532	14605
East Asia and Pacific	10422	10116	10414	11994	14704	17562
Central and South Asia	1668	2002	2251	2569	2987	3382
Middle East	332	451	511	606	810	923

ISO/IEC 27001 - Europe

Year	2012	2013	2014	2015	2016	2017
Country						
Spain	805	799	698	676	752	803

Se puede observar como en el sector de las tecnologías de la información se ha producido un gran incremento debido a que, este tipo de organizaciones poseen grandes cantidades de datos muy sensibles a que puedan salir a la luz, por lo que, este tipo de empresas deberían de tender a buscar este certificado, porque darán mayor grado de seguridad y confianza a sus clientes. Si no están certificados de esta norma por lo menos que esté implantada sería un buen comienzo:

ISO/IEC 27001 - Certificates by Industrial Sector

EA* Code Nos.	ISO/IEC 27001 BY INDUSTRIAL SECTOR	2012	2013	2014	2015	2016	2017
33	Information technology	4558	5059	4933	5573	6578	7478

5.11 ¿Qué dicen o cuentan las empresas certificadas?

Para conocer la experiencia de empresas ya certificadas, se mandaron varias encuestas a diferentes organizaciones de las cuales solo se obtuvieron dos contestaciones, una de S2 Grupo, empresa dedicada a la ciberseguridad y la segunda de Capgemini, dedicada a la consultoría, servicios tecnológicos y transformación digital. Ambas organizaciones están certificadas de las tres normas comentadas anteriormente. Se pueden observar las preguntas y sus respectivas contestaciones en el apartado 7.5 del Anexo.

Las empresas nos cuentan:

- Que buscan el certificado para conseguir mayor satisfacción del cliente y de terceros, por lo que se consigue un mayor prestigio externo.
- Que encontraron problemas a la hora de implementar las normas, en el caso de S2 Grupo al no estar algunos miembros implicados en el proyecto de implementación, cosa que se explica en el punto 4 de esta guía, donde hay que exponer todo correctamente a los empleados y resolverles cualquier duda que puedan tener del proyecto, dándoles a entender que son una parte fundamental para que el proyecto se pueda llevar a cabo. En el caso de Capgemini, los mayores problemas que han tenido es la poca madurez de la organización, para no tener problemas de este tipo lo mejor es informarse de la norma y contratar en el caso de ser necesario consultores externos.
- En que para abordar un proyecto de certificación se necesitará un equipo técnico con conocimientos de la norma en cuestión.
- La auditoría es una herramienta de mejora si se realiza de forma meticulosa y correctamente.
- Estas normas les han aportado grandes beneficios a las dos organizaciones y por lo tanto, es recomendable al menos implementarlas y si se cree necesario adquirir el certificado.

6.REFERENCIAS

1. Lic. Carlo M. Yáñez. Sistema de gestión de calidad en base a la Norma ISO 9001. *International eventos.* Artículo-Área de gestión. páginas 1-8.

2. Imagen PDCA. Página 4. PNG, 300 x 204, 34,1 KB. [Imagen digital en línea] [fecha de consulta 10 Mayo 2019]. Disponible en: **https://4improvement.one/es/knowledge/tools-techniques/24-problem-solving-tools/145-pdca**

3. Corinne N. Johnson. Los Beneficios del PDCA. *Quality Progress*, Editorial ProQuest. Milwaukee. Mayo 2002. Volumen 35, Nº5, página 120.

4. Wouter Van den Berghe. Aplicación de las normas ISO 9000 a la enseñanza y formación. *Formación profesional Nº15 Revista Europea*. Páginas 21-30, ca. 2000.

5. FRANCH LEON, Katia y GUERRA BRETANA, C. Rosa Mayelin. ISO 9000: una mirada desde la gestión del conocimiento, la información, innovación y el aprendizaje organizacional. *Cofin* [en línea]. 2016, vol.10, n.2, pp.29-54. ISSN 2073-6061.

6. Imagen ISO 9000. Página 5. PNG, 200 x 200, 69,5 KB. [Imagen digital en línea], [fecha de consulta 11 Mayo 2019]. Disponible en:

https://sites.google.com/site/portafolioingcalidad/home/normas-iso-9000

7. Bauset-Carbonell, María-Carmen y Rodenes-Adam, Manuel. Gestión de los servicios de tecnologías de la información: Modelos de aporte de valor basado en ITIL e ISO/IEC 20000. *El profesional de la información*, 2013, enero-febrero, v.22, n.1, páginas 54-61, ISSN:1386-6710.

8. Oltra Badenes, Raúl Francisco. *La norma ISO/IEC 20000. Finalidad y contenido*. Departamento de Organización de Empresas, Universitat Politècnica de València, 2017. [Fecha de consulta 17 de Abril 2019]. Disponible en: **http://hdl.handle.net/10251/84477**.

9. Imagen ISO 20000. Página 7. PNG, 320 x 157, 16,1 KB . [Imagen digital en línea], [fecha de consulta 14 Mayo 2019].Disponible en:

https://www.proactivanet.com/blog/itil/nueva-iso-20000-1-puntito-caramelo/

10. Alvarado Saavedra, Serguei. *Implantación de ISO 20000 en una PYME. Un modelo docente*[en línea]. Trabajo final de máster. Universidad de Extremadura, 2018. [Fecha de consulta 2 Junio 2019]. Disponible en: **http://hdl.handle.net/10662/7184**

11. Kempter, Stefan y Kempter, Andrea. *Beneficios ISO 20000*. 23 Agosto 2018 [Imagen digital en línea], [fecha de consulta 17 Mayo 2019]. Disponible en: **https://yasm.com/wiki/en/index.php/ISO_20000,** JPG, 1200 x 900, 155 KB.

12. Imagen ISO 20000. Página 8. JPEG, 200 x 157, 8 KB. [Imagen digital en línea], [fecha de consulta 14 Mayo 2019]. Disponible en:

https://definicion.de/tecnologia-de-la-informacion/

13. Bauset Carbonell, MDC. (2012). *Modelo de aporte de valor de la implantación de un sistema de gestión de servicios de TI (SGSIT), basado en los requisitos de la norma ISO/IEC 20000* [Tesis doctoral no publicada][Fecha de consulta 20 de Abril 2019]. Universitat Politècnica de València. Disponible en: **http://hdl.handle.net/10251/16546**.

14. Imagen ISO 27000. Página 9. PNG, 861 x 330, 104 KB. [Imagen digital en línea], [fecha de consulta 18 Mayo 2019]. Disponible en: **https://ostec.blog/es/generico/primeros-pasos-iso-27000**

15. Imagen ISO 27000. Página 10. PNG, 256 x 197, 92,5 KB. [Imagen digital en línea], [fecha de consulta 18 Mayo 2019]. Disponible en:

https://www.audea.com/es/servicios-combinados/ciberseguridad-al-alcance-todos/candado-062018/

16. Portal aenormas aenor [en línea], ISO 27001[fecha de consulta 20 Mayo 2019]. Disponible en:

https://portal.aenormas.aenor.com/aenor/Suscripciones/Personal/pagina_per_buscador.asp

17. Ladino A., Martha Isabel, Villa S., Paula Andrea, López E., Ana María, FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS. *Scientia Et Technica* [en línea] 2011, XVII, páginas 334-339. (Abril-Sin mes) : [Fecha de consulta: 25 Abril de 2019]. ISSN 0122-170. Disponible en:**<http://www.redalyc.org/articulo.oa?id=84921327061>**

18. W. Phillips, Ann. Auditorías de la calidad. *Cómo gestionar con éxito una auditoría interna conforme a ISO 9001:2015.* Aenor Internacional S.A.U. ISBN 978-8481439311.

19. Imagen auditoría. Página 11. JPG, 918 x 405 ,44,8 KB. [Imagen digital en línea], [fecha de consulta 19 Mayo 2019]. Disponible en: **https://seminarioiiuntref.wordpress.com/2015/11/12/importancia-de-la-auditoria-interna-en-las-organizaciones/**

20. Imagen auditoría. Página 12. PNG, 370 x 136, 46 KB. [Imagen digital en línea], [fecha de consulta 20 Abril 2019]. Disponible en:

https://auditest.es/auditorias-por-que-son-importantes-para-mi-empresa/

21. Gil Pechuán, I. (2010). Desarrollo de una auditoría de sistemas de información: Fases. En Riunet, [fecha de consulta 20 Mayo 2019]. Disponible en: **http://hdl.handle.net/10251/8372**

22. González-Reyes, Lisandra de la Luz, Moreno-Pino, Maira, Procedimiento para implementación de un sistema de gestión de costos de calidad. *Ciencias Holguín* [en línea] 2016, Vol.22, No.2, páginas 1-13 (Abril-Junio) : [Fecha de consulta: 1 de junio de 2019], ISSN 1027-2127. Disponible en:**<http://www.redalyc.org/articulo.oa?id=181545579002>**

23. Santillana, Juan Ramón. *Auditoría interna*. Pearson Educación de México, SA de CV, 2011. [Fecha de consulta 23 Abril 2019]. ISBN 9786073220460. Disponible en: **http://www.ingebook.com/ib/NPcd/IB_Escritorio_Visualizar?cod_primaria=1000193&libro=6199**

24. Imagen auditoría interna. Página 15. PNG, 297 x 169, 40,2 KB. [Imagen digital en línea], [fecha de consulta 24 Abril 2019]. Disponible en: **https://es.semrush.com/blog/realizar-auditoria-contenido-semrush/**

25. Padin, María Belén. *Auditoría externa: responsabilidades cuando se trabaja con otros profesionales.* Gestión Joven, vol. 2, Asociación Española de Contabilidad y Administración de Empresas, 2008, pp. 108–114 . ISSN 1988-9011. Disponible en: **https://doaj.org/article/c0a74cc100a745788459e7c80a07da8d**

26. Documento ENAC. CEA-ENAC-16 Rev.7. Certificación de Sistemas de Gestión de la Calidad y Ambiental. Criterios Específicos de Acreditación. Julio 2017 Serie 4.

27. Imagen Certificación. Página 16. PNG, 225 x 225, 4,95 KB. [Imagen digital en línea], [fecha de consulta 25 Mayo 2019]. Disponible en:

https://www.mediainteractiva.com/certificacion-propia/

28. Imagen auditoría externa. Página 17. JPG, 260 x 194, 7,82 KB. [Imagen digital en línea], [fecha de consulta 27 Abril 2019]. Disponible en:

http://tematicasanalisisydiagnostico.blogspot.com/2016/05/auditoria-externa.html

7.ANEXO

En este punto se va a ver información adicional al manual que puede resultar de interés para el lector.

7.1 Tecnologías de la información y comunicaciones

Las tecnologías de la información y comunicaciones(TICs) son las tecnologías necesarias para la gestión y transformación de la información, donde se usan sistemas informáticos y ordenadores que nos van a permitir modificar, proteger, almacenar, crear y recuperar la información.

La definición que nos aporta el Programa de las Naciones Unidas para el desarrollo nos dice que “las tecnologías de la información y comunicación se conciben en dos partes la tecnología de la comunicación basadas en todo aquello que nos permite transmitir y recibir información como son la radio, la televisión y los teléfonos, y por otra parte la tecnología de la información basada en los ordenadores, los equipos de telecomunicación y las interfaces”.

En la actualidad prácticamente todas las organizaciones utilizan sistemas informáticos para almacenar, crear, modificar o recuperar información por lo tanto, existen muchas empresas en el sector de las tecnologías de la información y comunicación.

7.2 Normas de la familia ISO 9000

Dentro de la familia ISO 9000 encontramos una serie de normas que se dividen en:

- ISO 9000: Principios fundamentales y vocabulario de calidad.
- ISO 9001: Es la única de esta familia de normas en la que una organización puede certificarse y es aquella que nos muestra la guía de sistema de gestión de calidad y sus requisitos.
- ISO 9004: Esta norma nos proporciona instrucciones para conseguir la mejora continua y mejora del desempeño.
- ISO 19011: Orientación en la empresa de las auditorías de sistemas de gestión de calidad.

7.3 Normas de la familia ISO 27000

El conjunto de normas que forman esta familia son:

- ISO 27001: Es la norma principal de esta serie de normas ya que incluye todos los requisitos de SGSI en las organizaciones. Es la más importante a la hora de certificarnos de esta serie de normas.
- ISO 27002: Es un manual de buenas prácticas donde se describen los objetivos de control y las evaluaciones recomendables de seguridad de la información. No es certificable.
- ISO 27003: Es un manual para implementar un SGSI y nos dará información necesaria para la utilización del ciclo PDCA comentado en el punto 2.2.1 y todos los requisitos de sus fases.
- ISO 27004: Se exponen las técnicas de medida y las métricas que podemos aplicar para determinar la eficacia de un SGSI y aquellos controles que estén relacionados.
- ISO 27005: Establece unas directrices para la gestión de los riesgos en la seguridad de la información.
- ISO 27006: Nos indica los requisitos para lograr la certificación y la acreditación de las entidades de la auditoría de SGSI.
- ISO 27007: Es un manual de la auditoría de un SGSI.
- ISO 27008: Guía para auditores de controles de seguridad de la información.
- ISO 27009: Aplicación norma 27001 a un sector en concreto. Los requisitos.
- ISO 27010: Gestión de la seguridad de la información en las comunicaciones intersectoriales e interorganizacionales.
- ISO 27011: Es una guía de gestión de seguridad de la información específica para telecomunicaciones.
- ISO 27013: Guía para la implementar íntegramente las normas ISO 27001 e ISO 20000-1
- ISO 27031: Guía que nos explica los principios y conceptos de la TIC.
- ISO 27032: Es un estándar que garantiza directrices de seguridad que según la organización ISO ayudará a reducir los riesgos en Internet.
- ISO 27033: Es una norma que deriva de la norma de seguridad ISO 18028 de la red y nos proporciona información general de seguridad de la red y diferentes conceptos.
- ISO 37034: Guía de seguridad en aplicaciones.
- ISO 27799: Es un estándar de SGSI dentro del sector sanitario, establece directrices necesarias para apoyar en la salud informática es un complemento a la norma ISO 27002.

7.4 Procesos de la normativa ISO 20000

Se dividen en 6 bloques:

- Portfolio de servicios
    - Prestación de servicios
    - Gestión de la configuración
    - Gestión de activos
    - Control de involucrados en el ciclo de vida d losl servicio
    - Gestión del catálogo de servicios
    - Planificación de servicios
- Aseguramiento de servicios:
    - Gestión de la seguridad de la información
    - Gestión de la disponibilidad y continuidad del Servicio
- Relación y acuerdo:
    - Gestión de proveedores
    - Gestión de nivel de servicio
    - Gestión de las relaciones con el negocio
- Diseño, transición y construcción de servicios:
    - Gestión de Cambios
    - Transición y diseño de servicios
    - Gestión del despliegue y la entrega
- Ejecución y resolución:
    - Gestión de problemas
    - Gestión de Incidencias y peticiones de servicio
- Oferta y demanda:
    - Gestión de la capacidad
    - Contabilidad y presupuesto de servicios
    - Gestión de la capacidad

7.5 Normas de la familia ISO 20000

La familia de normas que encontramos en esta familia ISO 20000 son las siguientes.

- ISO 20000-1: Es la norma más conocida de esta familia y es en la que se detallan los requisitos que debe de cumplir un sistema de gestión de Servicios de TI. Su última actualización se ha producido en el año 2018.
- ISO 20000-10: Describe los conceptos básicos y la terminología a la hora de utilizar la serie ISO 20000.
- ISO 20000-2: Son un conjunto de recomendaciones y buenas prácticas para facilitarnos el cumplimiento de los requisitos establecidos por lo que ayuda a comprender mejor la ISO 20000-1.
- ISO 20000-3: Es una guía para la definición del alcance y el ámbito de la aplicación de la ISO 20000-1.
- ISO 20000-4: Guía para elaborar un modelo de evaluación de procesos. Interesante para realizar una aproximación gradual a los requisitos de la ISO 20000-1.
- ISO 20000-5: Guía con sugerencias para la implantación del sistema de gestión de servicios de TI propuesto por la ISO 20000-1.

7.6 Encuestas a empresas certificadas

La primera encuesta que se puede ver es de **S2 Grupo** empresa dedicada a la ciberseguridad. Estas son sus respuestas:

ENCUESTA S2 GRUPO

1. ¿Su empresa está certificada en alguna de estas tres normas ISO? En caso afirmativo indique con una X de cual o cuales:

X	**9001:2015: Sistema de gestión de la calidad.**
X	**20000-1:2018: Sistema de gestión de servicios.**
X	**27001:2013: Sistema de gestión de la seguridad de la información.**

2. ¿Alguna de la norma o normas no señaladas anteriormente está en período de implementación o implementada?

Se encuentran todas implementadas hace años, si bien en los próximos meses abordaremos un proyecto interno de adaptación de nuestro SGSTI a la nueva versión de la norma ISO 20000-1.

3. En caso de estar implementada, ¿tienen previsto obtener el certificado de esta?

Las tres normas las tenemos certificadas con AENOR desde hace años.

4. ¿Puede indicar el motivo por el cual la organización se ha decidido a certificarse de la norma o normas señaladas en la primera pregunta?

9001:2015: Sistema de gestión de la calidad	**Mostrar a clientes y terceras partes el compromiso de S2 Grupo con la calidad y la seguridad mediante el cumplimiento de los requisitos de esta norma internacional.**
20000-1:2018: Sistema de gestión de servicios	**Mostrar a clientes y terceras partes el compromiso de S2 Grupo con la calidad y la seguridad mediante el cumplimiento de los requisitos de esta norma internacional.**
27001:2017: Sistema de gestión de la seguridad de la información	**Mostrar a clientes y terceras partes el compromiso de S2 Grupo con la calidad y la seguridad mediante el cumplimiento de los requisitos de esta norma internacional.**

5. ¿Qué dificultades encontraron en el proceso de implementación? Indíquelos diferenciando por normas.

En general para las tres normas: ninguna dificultad en el plano técnico; algunas dificultades en la implicación de algunas personas así como en la asignación y priorización de recursos para algunas tareas derivadas del cumplimiento de los requisitos de las distintas normas.

6. ¿Qué beneficios concretos le ha aportado a la empresa el estar certificado de estas normas?

9001:2015: Sistema de gestión de la calidad	**Reconocimiento externo.** **Más volumen de negocio en general. En concursos públicos: puntos adicionales o cumplimiento de requisitos obligatorios.**
20000-1:2018: Sistema de gestión de servicios	**Reconocimiento externo.** **Más volumen de negocio en general. En concursos públicos: puntos adicionales o cumplimiento de requisitos obligatorios.**
27001:2017: Sistema de gestión de la seguridad de la información	**Reconocimiento externo.** **Más volumen de negocio en general. En concursos públicos: puntos adicionales o cumplimiento de requisitos obligatorios.**

7. ¿Qué cree que necesita una empresa para acometer un proyecto de este tipo?

Primero un buen conocimiento técnico de los servicios ofrecidos así como del sector y de su entorno (mercado, competencia, legislación, tendencias, tecnologías...).

Y luego recursos con conocimiento técnico del sector y con experiencia y formación en gestión y en las normas de referencia.

8. ¿Considera los costes invertidos en la certificación un gasto o una inversión?

Inversión.

9. ¿Recomendaría a otras empresas del sector certificarse en estas mismas normas?

Lo que recomendaría sin dudarlo es su implementación.

Lo de certificarse o no depende de si hay una necesidad de real de ello, lo cual también depende a su vez del entorno y de las circunstancias.

10. ¿Considera las auditorías una herramienta de mejora o un requisito para tener el certificado?

Las auditorías internas, bien hechas, con tiempo y con rigor, son claramente una herramienta muy potente para la mejora.

Las auditorías externas de certificación en ocasiones también aportan información muy valiosa para la mejora; en otras ocasiones en absoluto. En éste último caso solo serían un requisito para obtener el certificado. El que la auditoría externa sea útil o no depende, como en el caso de las internas, del nivel, rigor y dedicación aportados por el auditor.

No se añadió ningún comentario más en el apartado final de "**otros comentarios que considere de interés apuntar**".

La segunda empresa que contestó a la encuesta es **Capgemini**, que es uno de los principales proveedores del mundo de consultoría, tecnología y transformación digital, las respuestas de Capgemini a la encuesta fueron las siguientes:

ENCUESTA CAPGEMINI

1. ¿Su empresa está certificada en alguna de estas tres normas ISO? En caso afirmativo indique con una X de cual o cuales:

X	**9001:2015: Sistema de gestión de la calidad.**
X	**20000-1:2018: Sistema de gestión de servicios. Pendiente de adecuación a la nueva versión de la norma ISO 20000-1; actualmente estamos certificados en ISO 20000-1:2011.**
X	**27001:2013: Sistema de gestión de la seguridad de la información.**

2. ¿Alguna de la norma o normas no señaladas anteriormente está en período de implementación o implementada?

Están implantadas y estamos certificados. Respecto a la ISO 20000-1, en la próxima auditoría externa, nos certificaremos en la nueva versión de la norma.

3. En caso de estar implementada, ¿tienen previsto obtener el certificado de esta?

NA

4. ¿Puede indicar el motivo por el cual la organización se ha decidido a certificarse de la norma o normas señaladas en la primera pregunta?

9001:2015: Sistema de gestión de la calidad	**Compromiso con la Calidad de los Servicios y la Satisfacción del Cliente.** **Certificado valorado por los clientes.**
20000-1:2018: Sistema de gestión de servicios	**Compromiso con la Calidad de los Servicios y la Satisfacción del Cliente.** **Certificado valorado por los clientes.**
27001:2017: Sistema de gestión de la seguridad de la información	**Compromiso con la Seguridad de la Información de la compañía, así como del grupo.** **Certificado valorado por los clientes.**

5. ¿Qué dificultades encontraron en el proceso de implementación? Indíquelos diferenciando por normas.

9001:

- **Fue la primera de todas, antes del 2000.**
- **Poca madurez de la compañía.**

20001:

- **Desconocimiento de cómo enfocar ciertos requisitos adicionales a la ISO 9001.**
- **Poca madurez en algunas áreas para dar cumplimiento a los requisitos.**

27001:

- **Poca cultura en Seguridad de la Información.**
- **Falta de involucración de personal clave.**

- **Falta de autonomía para implementar controles que afectan a la infraestructura IT globalizada.**
- **Falta de presupuesto para implementar controles con un mayor nivel de madurez.**

6. ¿Qué beneficios concretos le ha aportado a la empresa el estar certificado de estas normas?

9001:2015: Sistema de gestión de la calidad	**Fue la primera norma en la que nos certificamos y esta ha permitido tener una estructura de procesos y de cultura de compañía preparada para soportar el resto de las normas en la que nos hemos ido certificando durante los últimos años (20000-1, 27001, 14001, CMMI, etc.).**
20000-1:2018: Sistema de gestión de servicios	**Ha permitido tener un catálogo de servicios globales del área de servicios IT de la compañía y un nivel de madurez y control de los servicios superior a cualquier servicio certificado únicamente con la ISO 9001.**
27001:2017: Sistema de gestión de la seguridad de la información	**Nos permite impulsar nuevas iniciativas y mejoras manteniendo vivo el Sistema de Gestión de Seguridad de la Información.**

7. ¿Qué cree que necesita una empresa para acometer un proyecto de este tipo?

- **Alto compromiso de toda la Dirección.**
- **Presupuesto no solo para la certificación sino para abordar iniciativas de mejora que no únicamente sirvan para dar cumplimiento a los requisitos de las normas.**
- **Recursos humanos y técnicos adecuados y disponibles.**

8. ¿Considera los costes invertidos en la certificación un gasto o una inversión?

Esta respuesta seguramente dependerá de quien la responda. Pero desde nuestra área lo vemos como una inversión, se han impulsado e implementado iniciativas que si no fueran con la "excusa" de la certificación no se hubieran hecho. Es una herramienta que nos ayuda a mejorar y a impulsar iniciativas.

9. ¿Recomendaría a otras empresas del sector certificarse en estas mismas normas?

Sí, aunque incluiría alguna certificación ambiental (ISO 14001 o EMAS) y otra de seguridad laboral (ISO 45001 u OHSAS 18001).

10. ¿Considera las auditorías una herramienta de mejora o un requisito para tener el certificado?

Ambos. Lo segundo es obvio, si no realizas auditorías internas, no es posible mantener las certificaciones, aunque hay muchas formas de realizarlas y creo que en Capgemini vamos más allá de cumplir sólo con el requisito de norma.

En esta segunda encuesta tampoco se consideró aportar ningún comentario de interés en el apartado de "**Otros comentarios que considere de interés apuntar**".