UNIVERSIDAD GERARDO BARRIOS

SM-CRU

Datos Generales	
Facultad	Ciencia y Tecnología
Asignatura	Administración de Base de Datos II
Docentes	Beatriz Amaya, Beatriz Zuniga, Gisela Espinoza Oscar Torres
No. de Unidad	SEGURIDAD DE LOS DATOS
Contenido a desarrollar	Normas ISO para la seguridad de los datos

Introduccion

La gestión de seguridad de la información viene evolucionando desde sus albores como norma ISO-17799 del año 2000, hasta convertirse en la familia ISO 27000 desde el 2005 pretendiendo ser una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información. Esta norma está dirigida a los responsables de iniciar, implantar o mantener la seguridad de la información de una organización. La norma ISO 27001:2005 está orientada a establecer, implementar, operar, monitorear, analizar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información, SGSI y está alineada con la norma ISO 9001 con el fin de apoyar la implementación y operación, consistente e integrada con sistemas de gestión relacionados. Es decir, consolidar diversos sistemas de gestión de las organizaciones en uno sólo sistema integrado, optimizando sus procesos y facilitando el tránsito de información entre ellos. Recientemente, en octubre del 2013 se ha actualizado

la norma de requisitos del SGSI denominada ISO27001:2013 así como también la norma del Código de Práctica del Sistema de Gestión de Seguridad de la Información denominada ISO27002:2013. La edición 2013 de la norma ISO27001 proporciona un enfoque común y una estructura para las normas de los sistemas de gestión que se presta más fácilmente para la integración con otras normas de sistemas de gestión. La norma actualizada ISO-27001 cuenta con 114 controles en 14 categorías o dominios, en contraste con los 133 controles y 11 categorías contenidas en la edición 2005. Los requerimientos para el análisis de riesgos están alineados con la norma ISO 31000 para la gestión del riesgo. 22 [Gestión de la seguridad de la información] La norma ISO-27002 proporciona las directrices para las normas de seguridad de la información de la organización y las prácticas de gestión de seguridad de la información, incluyendo la selección, implementación y gestión de los controles, considerando el entorno de riesgos de seguridad de la información de la organización. El nuevo código de prácticas ha sido alineado, en cuanto al número de controles, con los de la norma ISO/IEC 27001, así como la terminología con la de la norma ISO/IEC 27000. Refleja la estructura del Anexo A de la norma ISO/IEC 27001:2013.

NORMAS ISO

Normas ISO para la seguridad de los datos

¿Qué es significa normas ISO?

¿Cuáles son las normas ISO para la seguridad de los datos?

Objetivo de la clase: Comprender los principios básicos de las normas ISO para la seguridad de los datos

Que Significa la norma ISO:

La norma ISO es establecida por la Organización Internacional de estándares (ISO), y se compone de estándares y guías relacionados con sistemas y herramientas específicas de gestión aplicables en cualquier tipo de organización.

Realmente es una entidad conocida a nivel global que publica normas internacionales asociadas a la calidad. En particular, las conocidas normas ISO son documentos en los que se especifican requerimientos que pueden ser utilizados en distintas instituciones para garantizar que sus productos y/o servicios cumplan con los objetivos de calidad deseada. Los beneficios de las normas ISO son notables permiten a las organizaciones reducir errores e incrementar la productividad minimizando de esta forma costos.

Cuáles son las normas ISO para la seguridad de los datos:

Inicialmente se debe de preguntar ¿Por qué preocuparse por la seguridad?

- Destrucción de la información y otros recursos.
- Modificación o distorsión de información.
- Robo, eliminación o pérdida de información u otros recursos.
- La revelación de información.

  La interrupción de los servicios.

La seguridad de la información incluye la protección de información, sistemas, recursos y demás activos contra desastres, errores (intencionales o no) y manipulación no autorizada, para reducir la probabilidad y el impacto de los incidentes de seguridad. De acuerdo con la norma ISO/IEC 27002:2007, la seguridad de la información es la protección de la información contra los diversos tipos de amenazas para garantizar la continuidad del negocio, minimizando los riesgos y maximizando el retorno sobre la inversión y las oportunidades de negocio. La seguridad de la información se obtiene como resultado de la implementación de un conjunto de controles, que comprenden políticas, procesos, procedimientos, estructuras organizacionales y funciones de hardware y software. En particular, los controles deben ser establecidos, implementados, monitoreados, evaluados y mejorados continuamente con el fin de cumplir con los objetivos del negocio y la seguridad de la organización. La identificación de los controles adecuados requiere una planificación detallada. A continuación, se especifican algunos conceptos:

- Incidente de seguridad: corresponde a cualquier evento adverso relacionado con la seguridad, por ejemplo, ataques de denegación de servicio (Denial of Service, DoS), robo de información, fuga y la obtención de un acceso no autorizado a la información.
- Activo: cualquier elemento que tenga valor para la organización y su negocio. Algunos ejemplos: bases de datos, software, equipos (computadores, notebooks), servidores, dispositivos de red (routers, switches, etc), personas, procesos y servicios.
- Amenaza: cualquier evento que explote vulnerabilidades. Causa potencial de un incidente no deseado, que puede resultar en daños a un sistema u organización (véase el punto 2.16 NTC ISO/IEC 27002:2007).
- Vulnerabilidad: cualquier debilidad que puede ser explotada y ponga en peligro la seguridad de los sistemas y datos. Fragilidad de un activo o

grupo de activos que pueden ser explotados por una o más amenazas. Las vulnerabilidades son fallas que permiten la aparición de deficiencias en la seguridad general del equipo o de la red. Configuraciones incorrectas en el equipo o en la seguridad también permiten la creación de vulnerabilidades. A partir de esta falla, las vulnerabilidades son explotadas por amenazas que cuando se materializan, causan daños al computador, a la organización o a los datos personales.

- Riesgo: combinación de la probabilidad (oportunidad de que la amenaza se materialice) de que ocurra un evento y sus consecuencias para la organización. Algo que puede ocurrir y sus efectos sobre los objetivos de la organización.
- Ataque: cualquier acción que comprometa la seguridad de una organización.
- Impacto: resultado evaluado de un evento en particular.

Preparando a la organización:

Antes de pensar en la gestión de la seguridad de la información en una organización, hay que tener en cuenta las respuestas a las siguientes preguntas:

- ¿Qué hay que proteger? Los activos de la organización requieren protección.
- ¿Contra qué o quién? ¿Cuáles son las amenazas que pueden afectar a la organización y cómo y quién puede explotar estas amenazas?
- ¿Cuál es la importancia de cada recurso? Cada recurso de la información participa en el proceso de negocio de la organización.

Elementos básicos de las normas ISO 27001 e ISO 27002

Existen la ISO 27001 como la ISO 27002, la ISO 27002 es mucho más detallada, mucho más precisa, entonces, pero no puede obtener la certificación ISO

27002 porque no es un estándar de gestión sino una guía detallada para comprender el proceso de certificación. La ISO 27001, define el sistema de gestión de seguridad de la información (SGSI); por lo tanto, es posible la certificación según ISO 27001. Este sistema de gestión significa que la seguridad de la información debe planificarse, implementarse, monitorearse, revisarse y mejorarse. Significa que la dirección tiene sus responsabilidades distintas, que se deben establecer, medir y revisar objetivos, que se deben realizar auditorías internas, etc. Todos esos elementos están definidos en ISO 27001. A continuación se presenta un resumen de las empresas certificadas en el mundo con ISO 27001

ISO/IEC 27001 se divide en 11 secciones más el anexo A; las secciones 0 a 3 son introductorias (y no son obligatorias para la implementación), mientras que las secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad. De acuerdo con el Anexo SL de las Directivas ISO/IEC de la Organización Internacional para la

Normalización, los títulos de las secciones de ISO 27001 son los mismos que en ISO 22301:2012, en la nueva ISO 9001:2015 y en otras normas de gestión, lo que permite integrar más fácilmente estas normas.

Sección 0 – Introducción: explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión. Sección 1 – Alcance: explica que esta norma es aplicable a cualquier tipo de organización.

Sección 2 – Referencias normativas: hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.

Sección 3 – Términos y definiciones: de nuevo, hace referencia a la norma ISO/IEC 27000.

Sección 4 – Contexto de la organización: esta sección es parte de la fase de planificación del ciclo PDCA (Planear, Hacer, Chequear y Actuar) y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI. Las 4 etapas del ciclo PDCA son: definición de los problemas, determinación de los objetivos, elección de los métodos, y preguntarse 5 veces porque se ha producido el problema.

Sección 5 – Liderazgo: esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

Sección 6 – Planificación: esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

Sección 7 – Apoyo: esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

Sección 8 – Funcionamiento: esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.

Sección 9 – Evaluación del desempeño: esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

Sección 10 – Mejora: esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Para implementar la norma ISO 27001 en una empresa, usted tiene que seguir estos 16 pasos:

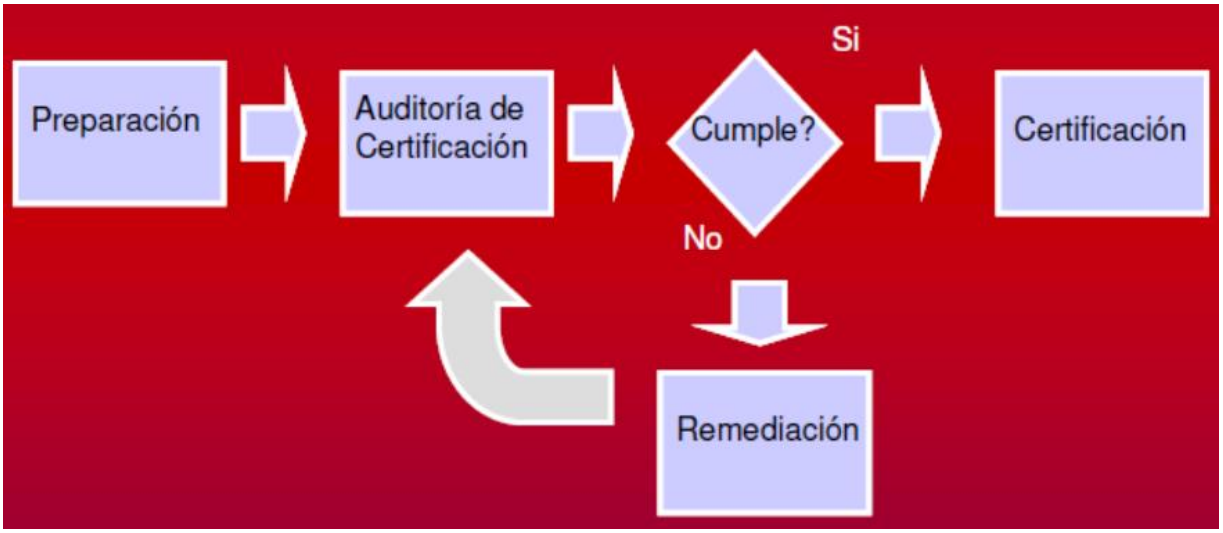
1. Obtener el apoyo de la dirección.
2. Utilizar una metodología para gestión de proyectos.
3. Definir el alcance del SGSI.
4. Redactar una política de alto nivel sobre seguridad de la información.
5. Definir la metodología de evaluación de riesgos.
6. Realizar la evaluación y el tratamiento de riesgos.
7. Redactar la declaración de aplicabilidad.
8. Redactar el Plan de tratamiento de riesgos.
9. Definir la forma de medir la efectividad de sus controles y de su SGSI.
10. Implementar todos los controles y procedimientos necesarios.
11. Implementar programas de capacitación y concienciación.
12. Realizar todas las operaciones diarias establecidas en la documentación de su SGSI.
13. Monitorear y medir su SGSI.
14. Realizar la auditoría interna.
15. Realizar la revisión por parte de la dirección.

16. Implementar medidas correctivas

Obtener la certificación.

Existen dos tipos de certificados ISO 27001: (a) para las organizaciones y (b) para las personas. Las organizaciones pueden obtener la certificación para demostrar que cumplen con todos los puntos obligatorios de la norma; las personas pueden hacer el curso y aprobar el examen para obtener el certificado. Para obtener la certificación como organización, se debe implementar la norma tal como se explicó y luego se debe aprobar la auditoría que realiza la entidad de certificación. La auditoría de certificación se realiza siguiendo estos pasos: • Primer paso de la auditoría (revisión de documentación): los auditores revisarán toda la documentación. • Segundo paso de la auditoría (auditoría principal): los auditores realizarán la auditoría in situ para comprobar si todas las actividades de una empresa cumplen con ISO 27001 y con la documentación del SGSI. • Visitas de supervisión: después de que se emitió el certificado, y durante su vigencia de 3 años, los auditores verificarán si la empresa mantiene su SGSI.

Etapas de certificación De manera general, en la siguiente figura se establecen las etapas que se requieren para alcanzar la certificación ISO 27001.



En la etapa de preparación, la empresa con todos sus recursos se alista para establecer el alcance de la certificación, en la siguiente etapa se realiza la propuesta de certificación, después se www.scprogress.com Página 37 determina si cumple o no, si no cumple con los requisitos, se ejecutan las acciones de remediación y nuevamente se analiza su cumplimiento, de ser positivo, se alcanza la certificación. El alcance de la certificación puede estar orientado a una unidad de negocios, una parte de la organización o el centro de procesamiento. Una vez definido el alcance se desarrolla un plan para obtener la certificación.

Ventajas seguridad de la información en una organización mediante un sistema de gestión

1 MEJORA CONTINUA

Gestionar la seguridad de la información supone establecer procesos específicos para la gestión que nos ayuden a: desarrollar una cultura de la seguridad en una empresa, implantar de forma gradual el control de la seguridad de la información y garantizar el crecimiento y la mejora continua de la Seguridad de la información

2 AJUSTARSE A LAS NECESIDADES DE CADA EMPRESA

Un sistema de gestión promueve el establecimiento de procesos de análisis de riesgos para la seguridad basados en la situación propia de cada organización y en la adopción de medidas adecuadas dentro de las posibilidades de cada empresa.

3 ESTABLECER CONTROLES ADECUADOS PARA LA SEGURIDAD DE LA INFORMACIÓN

Los controles para la seguridad de la información que se establezcan mediante la implantación de un sistema de gestión SGSI vendrán determinados por un análisis científico que permita evaluar cómo afectan a las necesidades de cada empresa las amenazas y riesgos de la seguridad de la información. Cada actividad y entorno en el que se desarrolla una actividad, así como el tamaño

y dimensión de cada organización determinara los controles adecuados para cada organización

Un sistema de Gestión SGSI basado en ISO 27001 también nos permitirá beneficiarnos de la adopción de las mejores prácticas del mercado y de la industria en todo el mundo para la seguridad de la información

4 INTEGRACIÓN DE SISTEMAS DE GESTIÓN

Un punto no menos importante es la integración del SGSI dentro de la gestión de la propia empresa.

Tipo de procesos: Existen 2 tipos de procesos en un SGSI para ISO27001 los cuales son:

1. Procesos de Gestión: Son propios del sistema de gestión básicamente enfocada a conseguir la revisión y mejora continua del sistema y que serán comunes a los procesos de gestión de calidad, medioambiente etc.

2. Procesos sobre la seguridad de la información

Procesos propios de la seguridad de la información que se integraran dentro de los procesos propios de cada actividad empresarial en conjunto con las demás dimensiones como la calidad o el medioambiente

Estructura de ISO 27001, está formada por 10 pasos principales:

1. OBJETO Y CAMPO DE APLICACIÓN. DEFINIENDO EL ALCANCE DEL SGSI: Pone al alcance de toda la gestión de la seguridad de la información y además a través de la certificación independiente ofrece la posibilidad a las pequeñas y medianas empresas de competir con empresas de mayor tamaño que pueden contar con sus propias herramientas de gestión.

2. REFERENCIAS NORMATIVAS: En este apartado se hace referencia a la norma ISO/IEC 27000 donde se nos ofrece una visión genérica sobre los sistemas de Gestión de la Seguridad de la Información (SGSI) y donde se nos habla entre otras cosas sobre la metodología base PDCA de todos los sistemas de Gestión

El ciclo PDCA de mejora continua, si bien en la versión 27001:2013 no se cita tan explícitamente como en versiones anteriores de la norma, constituye el marco fundamental sobre el que está construido el sistema de gestión SGSI.

3. TÉRMINOS Y DEFINICIONES: Con la finalidad de contar con una sola guía de términos y definiciones que sea consistente, dentro de la norma ISO 27001 se establecen las definiciones sobre el vocabulario fundamental referente a la seguridad de la Información que va a ser utilizado posteriormente en los requisitos de la norma. En la actual versión de la norma ISO 27001:2013 los términos y definiciones se encuentran referenciados en la sección 3 "Fundamento y vocabulario" de la norma ISO 27001:2013 donde se hace referencia a los términos y definiciones dados en el documento ISO 27000

4. CONTEXTO DE LA ORGANIZACIÓN: Conocer la organización y su contexto se plantea como un requisito de partida para poder establecer un punto de referencia en la aplicación del sistema de gestión de la seguridad de la información, se trata de que los objetivos en la seguridad de la información tengan en cuenta los propios objetivos del negocio de cada organización.

5. LIDERAZGO: Los requisitos relacionados con el liderazgo se refieren al compromiso que debe ejercer la dirección de la empresa en el proceso de implantación de un SGSI. En la revisión ISO 27001:2013 se considera como algo fundamental la implicación constante de la dirección en la implantación de una Cultura de la Seguridad en cada organización. El compromiso de la dirección se verifica con la aportación de los recursos tanto humanos como materiales para la consecución de los objetivos en la seguridad de la información.

6. PLANIFICACIÓN: Una vez identificadas las necesidades y expectativas de las partes interesadas tal como nos indica el punto 4 del contexto de la organización, deberemos establecer un plan definir los riesgos que debemos tratar y las actividades a realizar para mitigar o evitar dichos riesgos

7. SOPORTE: En este apartado la norma nos prescribe determinar los recursos necesarios para implementar los planes que hemos realizado en el apartado anterior 6. Planificación, siempre teniendo en cuenta el compromiso de la dirección en proveer los recursos necesarios.

8. OPERACIÓN: Se pone en marcha las medidas para la seguridad de la información que se han definido en los capítulos anteriores en concreto

9. EVALUACIÓN DEL DESEMPEÑO: Como parte fundamental de cualquier sistema de Gestión deberemos evaluar el desempeño de las acciones emprendidas.

10. MEJORA: La mejora del sistema de gestión de la seguridad de la información nos refiere a la actualización continua del sistema de gestión, esto incluye la revisión permanente para encontrar oportunidades de mejora aprendiendo por un lado de los errores cometidos.

Pasos Necesarios Para Implementar ISO 27001

Fase 1: Auditoria inicial ISO 27001 en base análisis GAP

Un análisis de brechas GAP es un método para evaluar las diferencias de rendimiento entre los sistemas de información de una empresa o las aplicaciones de software para determinar si se cumplen los requisitos del negocio y, de no ser así, qué pasos se deben tomar para garantizar que se cumplan con éxito. Gap se refiere al espacio entre "donde estamos" (el

presente) y "donde queremos estar" (el objetivo a alcanzar). Un análisis de deficiencias también puede denominarse análisis de necesidades, permitiéndonos determinar lo que nos falta y los recursos necesarios para alcanzar los objetivos.

Esta fase se trata pues de algo similar a una auditoria inicial por la que podemos tener una idea del GRADO DE IMPLANTACION de la norma eso 27001 en nuestra organización que nos puede servir para un doble objetivo primero para establecer el punto de partida para implementar la norma y evaluar el esfuerzo necesario así como tener una herramienta fiable para elaborar un plan de implementación de ISO 27001 y segundo mantener una herramienta de evaluación del grado de implantación de la norma durante el proceso de implantación y evaluar el grado de avance del proyecto

Fase 2: Análisis del contexto de la organización y determinación del alcance

Esta fase del proyecto consiste en establecer el contexto del SGSI en cumplimiento de los requisitos de la norma ISO 27001 recogidos en la cláusula 4 de la Norma "que trata del punto de partida para desarrollar el SGSI y consiste en determinar o identificar los "problemas" internos y externos a los que se enfrenta la organización".

Fase 3: Elaboración de la política. objetivos del SGSI

La política de seguridad como requisito de la norma ISO 27001 debe considerar en líneas generales los objetivos de la seguridad de la información de la empresa u organización. Para ello se debe de contentar las siguientes 2 preguntas: 1) ¿Qué queremos conseguir con la Seguridad de la información? Y 2) ¿Qué queremos conseguir con la Seguridad de la información?

Fase 4: planificación del SGSI

Esta etapa está formada por los siguientes documentos: Inventario de Activos, Catálogo de Amenazas, Valoración de las amenazas Para la Seguridad de la Información, Análisis de Riesgos, Evaluación de riesgos, Plan de tratamiento de riesgos, Selección de controles: Declaración de Aplicabilidad.

Fase 5: Documentación del SGSI

En esta parte se deja evidencia de todo el proceso y para ello se toma en cuenta dos aspectos importantes:

1) Garantizar la repetición en el tiempo de un proceso. La base para garantizar la aplicación sistemática de un proceso es su documentación

2) Establecer un proceso de mejora. La documentación de un proceso permite el acceso a la información valiosa cuando decidimos evaluar la eficacia de nuestro sistema de gestión y nos permite tomar decisiones para modificar por ejemplo el proceso de toma de decisiones para mejorar nuestro sistema. Este es uno de los principales motivos de un sistema de gestión: LA MEJORA CONTINUA de nuestros procesos

Fase 6: Implementando un SGSI

La fase de implementación del Sistema tiene como base la identificación de los controles de seguridad que hemos determinado en los capítulos anteriores, sobre todo en la identificación del contexto de la organización y en la determinación del alcance o aplicabilidad del SGSI. Es la hora de diseñar nuestros procesos de seguridad integrándolos en los procesos de nuestra organización tomando en cuenta los hallazgos identificados y los controles para mitigar los riesgos que deberemos poner en funcionamiento para

garantizar niveles aceptables en la confidencialidad, integridad y disponibilidad de la información.

Fase 7: Comunicación y sensibilización SGSI

Implantar un sistema de gestión de la seguridad de la información requiere de requisitos comunes relativos a los planes de comunicación comunes a cualquier programa que pretenda introducir cambios o mejoras en una organización

Fase 8: Auditoría interna según ISO 27001

Para cumplir con el requisito de la norma ISO 27001:_2013 deberemos establecer un plan de auditorías internas que nos permitan revisar el sistema de Gestión SGSI. Sin embargo, visto desde el punto de vista de la utilidad y no tanto del cumplimiento, la auditoría Interna se sitúa dentro del proceso de mejora continua, donde la auditoría interna es una de las herramientas más interesantes ya que nos permite identificar insuficiencias en el sistema y detectar potenciales situaciones de riesgo.

Fase 9: Revisión por la dirección según ISO 27001

La revisión del sistema de gestión es otro de los puntos clave dentro de la norma y que pudiera pasar desapercibido ya que a menudo no se le da la importancia que tiene realmente. Si tomamos este requisito como uno más del estándar y lo realizamos para cumplir solamente podríamos pasar por alto que este requisito es el que permite mantener vivo a un sistema de Gestión y permitir que el sistema de gestión cumpla con su verdadera función dentro de las buenas prácticas en seguridad de la información. Con más frecuencia de lo deseado nos encontramos con que esta revisión se hace solo para satisfacer al auditor de certificación, pero al hacerlo, se pierde una gran oportunidad

para que su alta dirección participe activamente en la seguridad de la información.

Fase 10: Proceso de certificación ISO 27001

El proceso de certificación de la norma ISO 27001 consiste en la obtención de un certificado de cumplimiento con los requisitos de la norma emitida por una entidad de certificación independiente. La norma bajo la que se obtiene el certificado es la norma UNE-EN ISO/IEC 27001. Las certificaciones emitidas por una Entidad de Certificación pueden ser o no acreditadas por una entidad de acreditación. En todo caso las entidades de acreditación deben pertenecer a la IAF (International Accreditation Forum). La fase de certificación no es obligatoria, pero tiene sin duda beneficios innegables a la hora de hacer valer la implantación de un SGSI ante nuestros clientes y partes interesadas.

ACTIVIDAD DE EVALUACIÓN DE LA SEMANA	
Nombre de la Actividad	ISO 27001 | ISO 27002
Tipo de Actividad	Tarea
Tipo de Participación	Equipo (3 integrantes)
Instrucciones para la actividad	Trabaje en forma colaborativa, definiendo equipos de trabajo de 3 estudiantes, garanticen como equipo que todos los integrantes participen explicando las normas ISO 27001-27002 realizando un análisis comparativo de las normas. La presentación deberá de desarrollarse durante el desarrollo de la clase práctica. Para el desarrollo de la presentación deberá utilizar una presentación en power point u otra herramienta de su preferencia; dicha presentación deberá ser compartida en el espacio de tarea correspondiente a la semana por un integrante del equipo.
Fecha de Entrega	Durante desarrollo de clase práctica
Ponderación	10% Laboratorio I

RECURSOS COMPLEMENTARIOS		
Web	Normas ISO 27001	https://normaiso27001.es/
Video	ISO 27001 Metodología	https://www.youtube.com/watch?v=d9HkY5gUO7A&t=148s
Video	ISO 27001: Cómo identificar riesgos de seguridad de la información	https://www.youtube.com/watch?v=d6qF80TB2bw