**Explica que comprende el estándar de gestión de seguridad ISO/IEC 27000**

Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044 con 27799 que indican las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un Sistema de Gestión de Seguridad de la Información (*SGSI*) basado en ISO 27001 en conjunto con otras normas de la serie 27000 pero también con otros sistemas de gestión.

**Por que ISO 27001 es importante para la empresa**

Hay 4 ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

* Cumplir con los requerimientos legales – cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001 ya que esta norma le proporciona una metodología perfecta para cumplir con todos ellos.
* Obtener una ventaja comercial – si su empresa obtiene la certificación y sus competidores no, es posible que usted obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.
* Menores costos – la filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos su empresa va a ahorrar mucho dinero. Y lo mejor de todo es que la inversión en ISO 27001 es mucho menor que el ahorro que obtendrá.
* Una mejor organización – en general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo. La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados.

**Como implementar ISO 27001**

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

* Obtener el apoyo de la dirección
* Utilizar una metodología para gestión de proyectos
* Definir el alcance del SGSI
* Redactar una política de alto nivel sobre seguridad de la información
* Definir la metodología de evaluación de riesgos
* Realizar la evaluación y el tratamiento de riesgos
* Redactar la Declaración de aplicabilidad
* Redactar el Plan de tratamiento de riesgos
* Definir la forma de medir la efectividad de sus controles y de su SGSI
* Implementar todos los controles y procedimientos necesarios
* Implementar programas de capacitación y concienciación
* Realizar todas las operaciones diarias establecidas en la documentación 4de su SGSI
* Monitorear y medir su SGSI
* Realizar la auditoría interna

**Qué es un SGSI**

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

**Para que sirve un SGSI**

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

**Como se implementa un SGSI**

se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

Plan: Establecer el SGSI

Do: Implementar y utilizar el SGSI

Check: Monitorizar y revisar el SDSI

Act: Mantener y mejorar el SGSIt

Cual es la parte central del SGSI

La confidencialidad, integridad y disponibilidad

**Que se considera un activo**

Los activos son los recursos del Sistema de Seguridad de la Información ISO 27001, necesarios para que la empresa funciones y consiga los objetivos que se ha propuesto la alta dirección.

Los activos tangibles son aquellos activos materiales que contienen información, y sobre los que tomaremos medidas preventivas para protegerlos principalmente de riesgos físicos: golpes, agua, fuego, etc. Los activos intangibles son aquellos que soportan la información dentro de un activo material, y pueden inutilizar la información, pese a que el activo físico no haya sufrido daño alguno.

**Que son los datos personales**

Los datos personales son cualquier información relativa a **una persona física viva identificada o identificable**. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal.

Los datos personales que hayan sido anonimizados, cifrados o presentados con un seudónimo, pero que puedan utilizarse para volver a identificar a una persona, siguen siendo datos personales y se inscriben en el ámbito de aplicación del RGPD.

**Que es un aviso de privacidad**

El **aviso de privacidad** es el documento por medio del cual se recaba el consentimiento de los titulares de los datos personales para dar tratamiento a los mismos y tú o tu empresa se comprometen a utilizar los datos recabados de manera responsable y segura, entre otros requisitos.

**Fases del sistema de gestión**

La norma ISO 27001 determina cómo gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información. Las fases son las siguientes:

* La Fase de planificación: esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad (la norma contiene un catálogo de 133 posibles controles).
* La Fase de implementación: esta fase implica la realización de todo lo planificado en la fase anterior.
* La Fase de revisión: el objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos “canales” y verificar si los resultados cumplen los objetivos establecidos.
* La Fase de mantenimiento y mejora: el objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.
* El ciclo de estas cuatro fases nunca termina, todas las actividades deben ser implementadas cíclicamente para mantener la eficacia del SGSI.