# Material - Seguridad de la Información

Material extraído del manual en línea que se encuentra en el siguiente link:

https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

# Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad

1 febrero, 2018
Sin categoría

## Confidencialidad, integridad y disponibilidad

La gestión de la información se fundamenta en tres pilares fundamentales que son, **confidencialidad, integridad y disponibilidad**. La seguridad de la información aplica barreras y procedimientos que **resguardan el acceso a los datos y sólo permite acceder a las personas** autorizadas para realizarlo.

La seguridad de la información se utiliza para **proteger los datos que tiene, maneja y dispone** una determinada organización. Las nuevas tecnologías han modificado la forma de utilizar la seguridad de la información a gran velocidad.

Las **sociedades avanzadas de nuestro tiempo se denominan**, sociedades de la información, ya que existe un enorme volumen de datos que son procesados, almacenados y transmitidos. Las organizaciones consideran que **la información es un**

**bien muy importante y se considera como prioritario**.  Se deberá gestionar de forma eficaz el almacenamiento, procesamiento y transmisión de la información. En otras palabras, **podemos decir que la información es poder**.

Existen diferentes definiciones del término seguridad de la información. De ellas nos **quedamos con la definición ofrecida por el estándar** para la seguridad de la información según la norma ISO 27001 por la Organización Internacional de Estandarización.

La seguridad informática consiste en la implementación de un conjunto de medidas técnicas **destinadas a preservar la confidencialidad, la integridad y la disponibilidad** de la información, pudiendo, además abarcar otras propiedades, como la autenticidad, la responsabilidad y la fiabilidad.

Existen tres principios que debe respetar la gestión de la información en cualquier empresa para **poder cumplir, de forma correcta, los criterios de eficiencia y eficacia**. Como algo general, se entiende que mantener un sistema seguro y fiable, es garantizar tres aspectos: confidencialidad, integridad y disponibilidad.

La **confidencialidad**, requiere que la información sea accesible de forma única a las personas que se encuentran autorizadas. Es **necesario acceder a la información mediante autorización y control**. La confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.

La gestión de la información se establece gracias a los tres pilares fundamentales

Es necesario determinar las empresas que a menudo desarrollan diseños que deben **proteger a sus competidores**.

La sostenibilidad de las organizaciones y su posicionamiento en el mercado pueden depender de forma directa a la implantación de los diseños y deben **protegerlos mediante mecanismos de control** de acceso que aseguren la confidencialidad de las informaciones.

El objetivo de la **confidencialidad** es, prevenir la divulgación **no autorizada de la información** sobre nuestra organización.

La **integridad**, supone que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá **modificar la información mediante autorización**.

El objetivo de la integridad es **prevenir modificaciones no autorizadas** de la información.

La disponibilidad supone que el sistema informático se mantenga trabajando sin sufrir ninguna **degradación en cuanto a accesos**. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información **deberá permanecer accesible a elementos autorizados**.

El objetivo es necesario **prevenir interrupciones no autorizadas** de los recursos informáticos.

La seguridad informática es un sistema que se encuentra disponible cuando el diseño o implantación **permite deliberar o negar el acceso a datos o servicios determinados**, es decir, un sistema que se encuentre disponible sin permite no estar disponible. Y un sistema que no se encuentra disponible es tan malo como no tener sistema.

Han crecido mucho los sistemas informáticos, en los diferentes ámbitos de la vida, lo que **ha incrementado el problema de los accesos no autorizados y la manipulación de los datos**. De ahí el gran valor que tiene para la información la confidencialidad, integridad y disponibilidad

El alto nivel de conectividad en el que nos encontramos hoy en día, no sólo proporciona **acceso en grandes cantidades y variedad de fuentes de datos** de forma cada vez mucho más rápido, además origina un aumento de las intrusiones de red.

Como es de vital importancia, es necesario conocer los diferentes ataques informáticos e intrusiones que existen, **dentro de la empresa y fuera**.  La seguridad de las tecnologías de información, **se convierte en un tema crucial para mejorar la importancia durante el avance** y el progreso de una empresa.

## Software ISO 27001

El estándar internacional **ISO 27001**, junto con todas las normas que componen su familia, generan todos los requisitos necesarios para poder implementar un **Sistema de Gestión de Seguridad de la Información** de una forma rápida y sencilla. Además el **Software ISOTools Excellence** para la **norma ISO 27001,** presta solución a todas estas cuestiones que se plantean a la hora de implementar un **Sistema de Gestión de Seguridad de la Información** en una empresa.

# Consejos básicos para implementar un Sistema de Gestión de Seguridad de la Información

8 junio, 2017

iso 27001:2013, SGSI

# Seguridad de la Información

La norma ISO 27001 ofrece los **requisitos básicos para implementar un Sistema de Gestión de Seguridad de la Información**.

Entendemos por información **todo el conjunto de datos organizados** en poder de una organización que poseen valor para la misma, independientemente de la forma en la que se guarde o **retrasmita su origen o fecha de elaboración**. Le recomendamos que lean ISO 27001: ¿Qué significa la Seguridad de la Información?.

La seguridad de la información, según la norma ISO 27001, consiste en **la preservación de la confidencialidad, integridad y disponibilidad**, además de los sistemas que se encuentran implicados en su tratamiento, dentro de la empresa.

## Consejos básicos

La **norma ISO 27001 puede ser implementada en las organizaciones para mejorar la seguridad de la información**. En el momento en el que se decide implementar la norma es importantes seguir todos estos consejos básicos:

- **Mantener la sencillez y restringir el alcance**. Un centro de trabajo, un proceso de negocio, un único centro de proceso de datos o un área sensible concreta, una vez que se ha conseguido el éxito y se han observado los beneficios, es necesario que se amplíe de forma gradual el alcance en diferentes fases.
- **Comprender los detalles que tiene el proceso de implementación**. Es necesario que se inicie en base a las cuestiones exclusivas técnicas, siendo un error sobrecargar de problemas la implementación. Es bueno adquirir experiencia de otras implementaciones, asistir a cursos de formación o contar con el asesoramiento de consultores externos especializados.
- **Gestionar el proyecto fijando los diferentes hitos con los objetivos y los resultados**.

- **La autoridad y el compromiso que ha tomado la dirección de la organización** evita las excusas para desarrollar las buenas prácticas, además de ser uno de los puntos fundamentales de la norma ISO 27001.
- **La certificación como objetivo**. Aunque se pueda conseguir la conformidad con la norma sin certificare. La certificación asegura un mejor enfoque, un objetivo mucho más claro y tangible y mejorar las opciones de conseguir el éxito. La certificación no debe ser la única meta. El principal objetivo es la gestión de la seguridad de la información que se alinea con el negocio.
- **No inventarse nada**. Es bueno apoyarse en los estándares, métodos y guías ya establecidos, además de la experiencia de otras empresas.
- **Utilizar lo que ya está implantado**. Pueden ser otros sistemas de gestión como ISO 9001, ISO 14001, OHSAS 18001, etc. que ya estén implementados en la empresa. Puede resultar útil como estructura de trabajo, ahorra tiempo y esfuerzo, además de crear sinergias. Es conveniente pedir ayuda e implicar a los responsables y auditores internos de otros sistemas de gestión.
- **Reservar la dedicación necesaria al día o a la semana**. El personal involucrado en el proyecto debe ser capaz de trabajar con continuidad en el proyecto.
- **Registrar evidencias**. Deben recogerse evidencias al menos tres meses antes de realizar la auditoría de certificación, para demostrar que el Sistema de Gestión de Seguridad de la Información funciona de forma correcta. No es bueno precipitarse a la hora de conseguir la certificación.
- **Mantener y mejorar de forma continua.** Es necesario considerar el mantenimiento y la mejora del Sistema de Gestión de Seguridad de la Información a lo largo del tiempo, esto supone que se requiere de esfuerzo y dedicación.

La seguridad de la información, consiste en la preservación de la confidencialidad

Click To Tweet

## Riesgos

Los riesgos a los que **se enfrentan a la hora de implementar un Sistema de Gestión de Seguridad de la Información** basado en la ISO 27001 son:

- Exceso de **tiempo de implementación**. Esto supone elevar los costes, desmotivación de los empleados, alejarse de los objetivos, etc.
- **Temor ante los cambios**. La resistencia de las personas.
- **Discrepancias en los comités** de dirección.
- Delegar **todas las responsabilidades en diferentes departamentos técnicos**.
- **No asumir que la seguridad de la información es inherente** a los procesos de negocio.
- Planes de **formación y concienciación**
- Calendario de revisiones que no se puedan cumplir.
- **No definir de forma clara al alcance.**
- Exceso de medidas técnicas en detrimento de la **formación, concienciación y medidas** de tipo organizativo.
- Falta de **comunicación de los progresos** al personal de la empresa.

## Factores de éxito

Los **factores de éxito de implementar** la norma ISO 27001 son los siguientes:

- La **concienciación de los trabajadores** por la seguridad. Es el principal objetivo que se quiere conseguir.
- Realizar los **comités a diferentes niveles** con gestión continua de no conformidades, incidentes de seguridad, acciones de mejora, tratamiento de riesgos, etc.
- Crear un **sistema de gestión de incidentes** que recoja todas las notificaciones continuas por parte de los usuarios.
- La **seguridad absoluta no existe**, por lo que la implementación de la norma lo que pretende es reducir el riesgos aniveles aceptables.
- La **seguridad no es un producto**, es un proceso.
- La **seguridad no es un proyecto**, es una actividad continua y un programa de protección requiere de un soporte de la empresa para tener éxito.
- La **seguridad debe ser inherente** a los procesos de información y del negocio.

# Software ISO 27001

El estándar internacional **ISO 27001 2013**, junto con todas las normas que componen su familia, generan todos los requisitos necesarios para poder implementar un **SGSI** de una forma rápida y sencilla, además el **Software ISOTools Excellence** para la **norma ISO 27001 2013** presta solución a todas estas cuestiones que se plantean a la hora de implementar un **SGSI** en una empresa.