La norma ISO 27002 complemento para la ISO 27001

ISO 27002

Cuando se habla sobre la **seguridad de la información nos viene a la cabeza la norma** ISO 27001. Esta norma es muy relevante dentro del sector ya que, toma como base todos los riesgos a los que se enfrenta la organización en su día a día, tiene como **objetivo principal establecer, implantar, mantener y mejorar** de forma continua la seguridad de la información de la organización. Sin embargo, no debemos olvidar el papel que ocupan otras normas.

En este caso la norma ISO 27002 de la que hablaremos en este post y que establece un **catálogo de buenas prácticas** que determina, desde la experiencia, una serie de objetivos de control y controles que se integran dentro de todos los requisitos de la **norma ISO 27001 en relación con el tratamiento de los riesgos**.

La importancia de disponer de una actualizada, completa y veraz información es la clave para la correcta realización de todas las actividades de la organización, en todas sus áreas, campos y actividades. Sin embargo, es todavía **mucho más importante mantener dicha información con seguridad** para que no se pierda, se robe o se deteriore de cualquier forma. Al fin y al cabo, la información y los datos de los que se dispone en la organización y que **recopila en su día son uno de los activos más valiosos** que pueden marcar el futuro de la organización.

De esta manera, es fácil comprender la importancia de la norma ISO 27001 como Sistema de Gestión de Seguridad de la Información. Sin embargo, es igual de importante el papel que **ocupa dentro de todos los requisitos de la norma ISO 27002** como guía de buenas prácticas para implantar controles y que garantizarán la seguridad de la información gracias a sus recomendaciones.

La norma **ISO 27002 se encuentra estructurada en 14 capítulos** que describen las áreas que se deben considerar para garantizar la seguridad de la información de las que se dispone. El documento recomienda un total de 114 controles, si bien no **hace falta cumplirlos todos**, sí que hay que tenerlos en cuenta y considerar su posible aplicación, además del grado de la misma.

Queremos **realizar una revisión muy breve** de cada uno de los 14 capítulos.

1 Políticas de Seguridad de la Información

Dentro de este capítulo se hace hincapié en la importancia que ocupa la disposición de una **adecuada política de seguridad**, aprobada por la dirección, comunicada a todo el personal, revisada de forma periódica y actualizada con los cambios que se producen en el interior y en el exterior.

2 Organización de la Seguridad de la Información

Los controles indicados en este capítulo buscan **estructurar un marco de seguridad** eficiente tanto mediante los roles, tareas, seguridad, etc. como en los dispositivos móviles.

Tenemos que tener presente que cada vez es mayor el peso que está ocupando el teletrabajo dentro de las empresas, y por ello, se deben tener en cuenta **todas sus características especiales** para que ningún momento la seguridad de la información de la que se dispone se vea afectada.

3 Seguridad relativa a los recursos humanos

Si analizamos los incidentes de seguridad que se producen en una organización nos daremos cuenta de que **la gran mayoría de estos tienen su origen en un error humano**. Se debe concienciar y formar al personal de los términos de empleo de la información en el desarrollo de sus actividades y la importancia que tiene la información en el desarrollo de sus actividades, además de la importancia que tiene promover, mantener y mejorar **el nivel de seguridad adecuándolo a las características** de los datos y la información que maneja es clave y uno de los objetivos que se debe perseguir.

4 Gestión de activos

Se centra en la atención en la **información como activo** y en cómo se deben establecer las medidas adecuadas para guardarlos de las incidencias, quiebras en la **seguridad y en la alteración no deseada**.

5 Control de acceso

Controlar quien accede a la información dentro de un aspecto relevante. Al fin y al cabo no todas las **personas de una organización** necesitan acceder para realizar su actividad diarias a todos los datos, sino que tendremos roles que **necesitan un mayor acceso** y otros con un acceso mucho más limitado. Para poder marcar las diferencias, se deben establecer todos los controles como registro de los usuarios, **gestión de los privilegios de acceso**, etc. siendo algunos de los controles que se incluyen en este apartado.

6 Criptografía

En el caso de que estemos **tratando la información sensible o crítica** puede ser interesante utilizar diferentes técnicas criptográficas para **proteger y garantizar** su autenticidad, confidencialidad e integridad.

7 Seguridad física y del entorno

La seguridad no es solo a nivel tecnológico sino también físico, es decir, una simple labor de no dejar las pantallas e impresoras en zonas que sean fácilmente accesibles, por parte del personal externo los documentos con los que se están trabajando no sólo nos permitirán gestionar de forma adecuada la seguridad sino que se **acabarán convirtiendo en hábitos que nos aportan eficiencia** en la gestión.

8 Seguridad de las operaciones

Tiene un marcado componente técnico entrado en todos los **aspectos disponibles como la protección** del software malicioso, copias de seguridad, control de software en explotación, gestión de vulnerabilidad, etc.

9 Seguridad de las comunicaciones

Partiendo de la base de que la gran mayoría de los intercambios de información y de datos en distintas escalas **se llevan a cabo mediante las redes sociales**, garantizar la seguridad y proteger de forma adecuada los medios de transmisión de estos datos clave.

10 Adquisiciones, desarrollo y mantenimiento de los sistemas de información

La seguridad no es un aspecto de un área en concreto, ni de un determinado proceso, no que es general, **abarca toda la organización** y tiene que estar presente como elemento transversal clave dentro del ciclo de vida del sistema de gestión.

11 Relación de proveedores

Cuando se establecen las relaciones con terceras partes, como puede ser proveedores, se deben **establecer medidas de seguridad** pudiendo ser muy recomendable e incluso necesario en determinados casos.

12 Gestión de incidentes de seguridad de la información

No podemos hablar de **controles de seguridad** sin mencionar un elemento clave, los incidentes en seguridad. Y es que, estar preparados para cuando estos incidentes ocurran, dando **una respuesta rápida y eficiente** siendo la calve para prevenirlos en el futuro.

13 Aspectos de seguridad de la información para la gestión de la continuidad de negocio

No sabemos lo que necesitábamos un dato hasta que lo hemos perdido. Sufrir una pérdida de **información relevante y no poder recuperarla** de laguna forma puede poner

en peligro la continuidad de negocio de la organización.

14 Cumplimiento

No podemos hablar de seguridad de la información, sin hablar de legislación, normas y políticas aplicables que **se encuentre relacionadas con este campo** y con las que conviven en las organizaciones. Debemos tener presente que ocupan un enorme lugar en cualquier sistema de gestión y deben **garantizar que se cumple** y que están actualizados con los últimos cambios siendo esencial para no llevarnos sorpresas desagradables.

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 **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.

(**3** votes, average: **4,67** out of 5)

Cargando...

ISO 27001

dad de la

Seguridad de

a los

del entorno

peraciones

sarrollo y
s sistemas...

edores

ntes de
nación

ridad de la
estión de l...

PRINT