Norma ISO 27001

¿Qué es la ISO 27001?

Sistemas de Gestión la Seguridad de la Información

ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar **ISO 27001:2013** para los **Sistemas Gestión de la Seguridad de la Información** permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de **ISO-27001** significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

La **Gestión de la Seguridad de la Información** se complementa con las buenas prácticas o controles establecidos en la norma **ISO 27002**.

Estructura de la norma ISO 27001

1. Objeto y campo de aplicación: La norma comienza aportando unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar.
2. Referencias Normativas: Recomienda la consulta de ciertos documentos indispensables para la aplicación de **ISO27001**.
3. Términos y Definiciones: Describe la terminología aplicable a este estándar.
4. Contexto de la Organización: Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del **SGSI**.
5. Liderazgo: Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma.
6. Planificación: Esta es una sección que pone de manifiesto la importancia de la determinación de riesgos y oportunidades a la hora de planificar un **Sistema de Gestión de Seguridad de la Información**, así como de establecer objetivos de **Seguridad de la Información** y el modo de lograrlos.
7. Soporte: En esta cláusula la norma señala que para el buen funcionamiento del **SGSI** la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso.
8. Operación: Para cumplir con los requisitos de **Seguridad de la Información**, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la **Seguridad de la Información** y un tratamiento de ellos.

9. Evaluación del Desempeño: En este punto se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del **Sistema de Gestión de Seguridad de la Información**, para asegurar que funciona según lo planificado.
10. Mejora: Por último, en la sección décima vamos a encontrar las obligaciones que tendrá una organización cuando encuentre una no conformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del **SGSI**.

Novedades de la ISO 27001:2013

Esta norma fue publicada recientemente, aportó una serie de cambios con respecto a su antecesora que los usuarios de los **SGSI** tienen que asimilar para continuar gestionando de forma eficaz la **Seguridad de la Información**. Las novedades que manifiesta son:

- No aparece la sección "Enfoque a procesos" con su respectiva metodología basada en el ciclo **PHVA**, ahora ofrece mayor flexibilidad.
- Se elimina la obligatoriedad de algunos documentos, conservando únicamente la declaración de aplicabilidad.
- Se han revisado los requisitos y controles.
- Se apuesta por un enfoque del análisis del riesgo en la fase de planificación y operación.

¿Por qué ISO 27001 es importante para su 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 l

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.

Referencia bibliográfica

Lectura 4

SEGOVIA, A. J. S. ANTONIO. (s.f.). NORMA ISO 27001. Recuperado 27 octubre, 2018, de https://advisera.com/27001academy/es/que-es-iso-27001/