

# ISO/IEC 27001

## Information Security Management Systems

La administración, la industria, los ciudadanos y la sociedad confían en muchas infraestructuras críticas (Ej. energía, abastecimiento de agua, transporte, industria, sector financiero, telecomunicaciones y servicios sanitarios). La necesidad de asegurar la continuidad en el funcionamiento de estas infraestructuras es básica. La seguridad de la información es un aspecto crítico.

La información es un activo fundamental de cualquier negocio y se extiende desde la información digital o los documentos de papel, los activos físicos (ordenadores y redes) o el mismo conocimiento de los empleados. Los acontecimientos que afectan la integridad, el secreto y la disponibilidad de información pueden afectar a la continuidad de una empresa, al poder afectar tanto a sus finanzas como su credibilidad. En EEUU según la encuesta sobre delito informático y seguridad de CSI/FBI, la estimación de pérdidas causadas en un año por los diferentes incidentes en seguridad informática superaron los 50 millones de dólares. En España la Ley Orgánica 15/1999, de protección de datos personales, la Ley 8/11, de protección de infraestructuras críticas y otros requisitos legales implican fuertes responsabilidades a las organizaciones.

La seguridad de la información se define como la preservación de la confidencialidad, la integridad y la disponibilidad de información. La norma ISO/IEC 27001 es un estándar internacional que especifica los requisitos para establecer, implantar, poner a funcionar, supervisar, revisar, analizar indicadores, mantener y mejorar un sistema de gestión documentado de la seguridad de la información dentro del contexto de los riesgos totales del negocio de la organización. También proporciona un marco para implantar algunos de los principios de la OCDE (Organización para la Cooperación y el Desarrollo Económico), pautas para la seguridad de los Sistemas y Redes de Información usando el modelo de mejora continua PHVA (Planificar-Hacer-Verificar-Actuar) y el enfoque en procesos.

La norma ISO/IEC 27001 está en concordancia con otros estándares internacionales para Sistemas de Gestión como ISO 9001 para los Sistemas de Gestión de Calidad e ISO 14001 para los Sistemas de Gestión Ambiental o la ISO 28000 para Sistemas de Gestión de Seguridad en la Cadena de Suministro.

Algunos de los requisitos comunes a estas normas son:

- Establecimiento de políticas y objetivos
- Supervisión, revisión y actividades de mejora
- Formación, toma de conciencia y competencia
- Las auditorías internas y la revisión por la dirección

Además, esta norma define su alcance en cuanto al grado de riesgo; identificación, análisis y evaluación de riesgos; identificación y evaluación de soluciones para eliminar riesgos y selección de los controles objetivo y controles para los riesgos identificados.

ABS Quality Evaluations (ABS QE) tiene un equipo de auditores altamente cualificados en sistemas de gestión, preparados para realizar evaluaciones de Sistemas de Gestión de Seguridad de la Información según los requisitos de la norma ISO/IEC 27001.

### ¿Quién necesita esta certificación?

La norma ISO/IEC 27001 puede aplicarse a cualquier tipo de organización que desee:

- Credibilidad, confianza y fiabilidad de sus clientes
- Ahorro económico por accesos indebidos a información
- Cumplimiento de la legislación
- Compromiso a todos los niveles de la empresa

Hay un interés inicial de aplicar esta norma desde una amplia gama de actividades, incluyendo: compañías de telecomunicaciones, tecnologías de la información, financieras, sanitarias, públicas y otras infraestructuras críticas que usan bases de datos personales, así como ingenierías, industrias petroquímicas, electrónica e instrumental, de fabricación manufacturera y de maquinaria y todas las Pymes en general.

# ABS Quality Evaluations

AN ABS GROUP COMPANY

### Para más información:

ABS Quality Evaluations

Calle Orense, 34 – 10º – C.P.: 28020 – Madrid

Gran Vía nº 630, 4ª – C.P.: 08007 – Barcelona

Tel: + 34 915552562 / + 34 934920458

Email: [info-es@abs-qe.com](mailto:info-es@abs-qe.com)

[www.abs-qe.com](http://www.abs-qe.com)