NORMAS, ESTANDARES, MARCOS

Normas

Organizaciones como ISO, IEEE, AENOR, NIST y otras, desarrollan y publican normas nacionales e internacionales. Las normas son acuerdos de expertos. Son como una fórmula que describe la mejor manera de hacer ciertas actividades, ya sea para la fabricación de un producto, la gestión de un proceso, la prestación de un servicio o el suministro de equipos.

En Ecuador, el INEN adapta y/o desarrolla normas para diversas actividades productivas y profesionales (Ver www.normalizacion.gob.ec), incluyendo a las TIC.

Las normas se basan en el conocimiento de expertos en el campo elegido, conscientes de las necesidades de las organizaciones que representan, ya sean fabricantes, distribuidores, compradores, usuarios, asociaciones profesionales, consumidores u organismos reguladores.

Por ejemplo:

- Las normas para la gestión de la calidad de trabajo de manera más eficiente y reducir los productos defectuosos.
- Las normas sobre gestión ambiental para reducir los impactos ambientales, reducir los residuos y adoptar un enfoque más sostenible.
- Las normas de salud y seguridad para prevenir accidentes en el lugar de trabajo.
- Las normas de gestión de la energía para reducir el consumo de energía.
- Las normas de seguridad de los alimentos para evitar la contaminación del producto.
- Los estándares de seguridad de la información para garantizar la seguridad de la información sensible.
- Las normas y estándares para desarrollo de software

Estándares

Son normas que cumplen algunas condiciones:

- Son certificables mediante una auditoria especializada. Igualmente, pueden existir Certificaciones personales acerca de su Auditoria.
  Ejemplo: ISO 27001 puede servir para la certificación de un Sistema de Gestión de Seguridad de la Información (SGSI) institucional. Adicionalmente, las personas pueden obtener una Certificación como Auditores ISO 27001
- Se refieren a requerimientos de los sistemas.
  Ej: ISO 27001, ISO 22301
- Mantienen una estructura de cláusulas y sub-clausulas. Generalmente, las primeras son de información general. Las demás son de carácter especifico
- En el caso de ISO, las Cláusulas reflejan el modelo de solución de problemas Plan-Do-Check-Act (PDCA)

Buenas Practicas (Best Practices) y Marcos (Frameworks)

Son normas que:

- **Marcos**: Establecen un conjunto organizado y sistemático de procesos, procedimientos y actividades no obligatorias, para mejorar el desarrollo de productos y servicios.
  Ej: COBIT, ITIL

- **Buenas Practicas:** Detallan o complementan un estándar.
  Ej. ISO 27002 detalla los Controles del Apéndice A de ISO 27001

- Generalmente, no son certificables, pero las personas pueden obtener una o más Certificaciones de una jerarquía a disposición.

Ejemplo: ISO 27001

Plan: Planeación. Cláusulas 4, 5, 6
Do: Ejecución. Cláusulas 7,8
Check: Evaluación. Cláusula 9
Act: Mejora Continua. Cláusula 10

Contents Page

Ciclo PDCA de ISO 27001: