1. Normativa/Marco referencial Nacional

Norma Técnica Peruana NTP-ISO/IEC 17799:2007 (NTP, 2007)

Reseña:

Esta norma ha sido elaborada por el Comité Técnico de Normalización de Codificación e Intercambia Electrónico de Datos (EDI), utilizando como antecedente a la Norma ISO/IEC 17799:2007 Information technology – Code of practice for information security management y en la que participaron empresas privadas, entidades públicas e instituciones educativas de renombre a nivel nacional como la Pontificia Universidad Católica del Perú, E. Wong S.A. y la Presidencia del Consejo de Ministros; por citar algunos.

- ✓ Objeto y Campo de Aplicación:

  Esta norma ofrece recomendaciones para realizar la gestión de seguridad de la información que puede utilizarse por los responsables de iniciar, implantar o mantener y mejorar la seguridad en una organización.

  Persigue proporcionar una base común para desarrollar normas de una seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad. La norma puede servir como una guía práctica para desarrollar estándares organizacionales de seguridad y prácticas efectivas de la gestión de seguridad. Las recomendaciones que se establecen en esta norma deberían elegirse y utilizarse de acuerdo con la legislación aplicable en la materia.

- ✓ Estructura de la norma:

  Esta norma contiene 11 cláusulas de control de seguridad que contienen colectivamente un total de 39 categorías principales de seguridad y una cláusula introductoria conteniendo temas de evaluación y tratamiento del riesgo.

- ✓ Clausulas:

  Cada cláusula contiene un número de categorías principales de seguridad. Las 11 cláusulas (acompañadas por el número de categorías principales de seguridad incluidas en cada cláusula) son:

  a) Política de seguridad (1).
  b) Aspectos organizativos para la seguridad (2).
  c) Clasificación y control de activos (2).
  d) Seguridad en recursos humanos (3).
  e) Seguridad física y del entorno (2).
  f) Gestión de comunicaciones y operaciones (10).

g) Control de acceso (7).

h) Adquisición, desarrollo y mantenimiento de sistemas de información (6).

i) Gestión de incidentes en la seguridad de la información (2).

j) Gestión de la continuidad del negocio (1).