Tema 4

Especificaciones de calidad y certificaciones

Ejercicio Profesional de la Informática

Contenidos

- Calidad en el tratamiento de la información y en el software
- Principales normas y certificados de calidad en TIC (Tecnologías de la Información y la Comunicación)
  - Iso 9000-9001
  - Calidad en el software
    - Iso 15504 (Spice)
    - Iso 25000 (Square)
    - CMMI
  - Tratamiento de la información (TIC)
    - Iso 20000
    - Iso 27000

Introducción

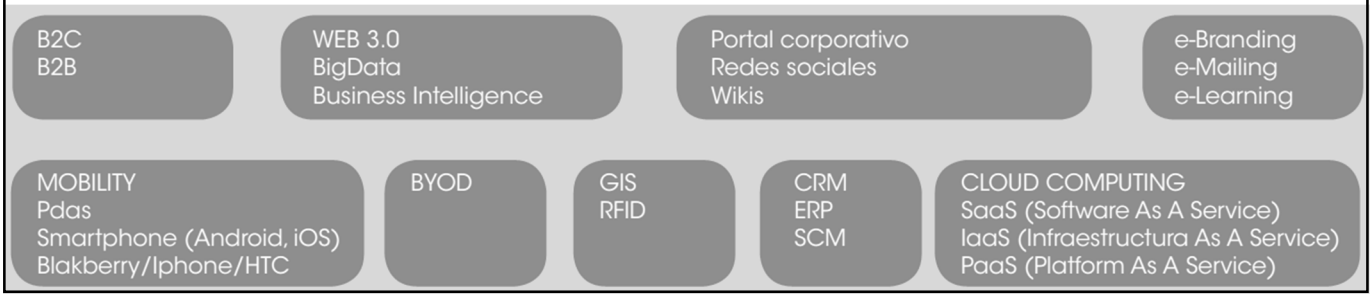
- Hay muchas formas de conseguir la calidad a todos los niveles (TIC, software, gestión de la empresa, etc.)
  - En este tema nos centramos en estándares internacionales
  - Sirven como guía de implementación y organización
- Las normas de calidad nacen para que las empresas se rijan por unos principios de organización y para que den estabilidad en el mercado y en la sociedad
  - También sirven para conseguir certificaciones oficiales y fomentar la confianza B2C (Business to Client) y B2B (Business to Business)
  - Aumentan mucho el prestigio de la empresa

Introducción

- Como informáticos nos interesan dos tipos de normativa (al margen de las leyes de obligado cumplimiento):
  - La relacionada con el desarrollo de software (Ingeniería del Software)
    - Parte pura de software: Iso 15504, Iso 25000, etc.
  - La relacionada con el tratamiento de la información en TIC
    - Parte común a muchas disciplinas tecnológicas y a la propia gestión de la empresa: Iso 9001, Iso 20000, Iso 27000, etc.
- Todas estas normas y estándares son de cumplimiento voluntario
  - No obstante ayudan mucho porque son métodos contrastados que funcionan
  - La empresa logra sus objetivos legales, de prestigio y de imagen
  - Las grandes empresas suelen aplicarlas siempre que es posible

Introducción

- Además del desarrollo de software nos interesa todo el tratamiento de información de la empresa
  - Nuevos negocios y nuevas herramientas en TIC
  - La información hoy en día es casi toda digital
  - Los informáticos estamos involucrados no sólo en hacer software sino también en el mantenimiento, auditorías, formación, etc.



Introducción

- Los cargos más importantes en la empresa afectados por las TICs
  - CEO (Chief Executive Officer ó Director General)
    - Si la empresa es de TIC es probable que también tenga formación en informática
  - CIO (Chief Information Officer ó Director de Informática)
    - Debe tener conocimientos avanzados en informática

Calidad en el software

- Dentro de la **Ingeniería del Software** podemos adoptar la definición de ***Calidad*** de la norma ISO-8402, y otras (p. ej: ISO-14598):

  "La totalidad de aspectos y características de un producto o servicio que tienen que ver con su habilidad para satisfacer las necesidades declaradas o implícitas"

- La calidad es un objetivo importante para cualquier producto software
  - No obstante el software **se construye para ser utilizado**
  - El principal objetivo de un producto es satisfacer necesidades de los usuarios
  - La calidad no es el objetivo último del producto, pero sí es importante
- La calidad de un producto software **no se puede referir únicamente a obtener un producto sin errores**

Calidad en el software

- La especificación de la calidad del software debe ser más detallada y exacta, y el camino para ello es su formalización mediante un modelo de gestión
- El mundo del desarrollo de software (como servicio TIC) necesita una supervisión constante por parte de profesionales para mantenerlo actualizado y en condiciones de funcionamiento
- Hay certificaciones (ej: ISO 15504) que proporcionan a las organizaciones un planteamiento estructurado para ofrecer y desarrollar servicios de aplicaciones software fiables

Calidad en el software

- La certificación es un reto, pero también es una oportunidad que tienen las empresas para generar más clientes y abrirse a nuevos mercados
- Existen diversos modelos de calidad en el ámbito del software
  - Sistemas de gestión
  - Calidad en el producto software
  - Calidad en los procesos software

Calidad en el software

- Normalmente las normativas son conjuntos de buenas practicas que se aplican sobre el ciclo de vida de proyectos informáticos y que contribuyen a mejorar los factores de la calidad del software
  - Algunas empresas de desarrollo de software han implantado sistemas de gestión basados en ISO 9001, ISO 27001 o ISO 20000 con alcances en los procesos de desarrollo y entrega
- Enfoque hacia los clientes
  - Tanto enfoque interno en la empresa como externo
  - En Software es mejor hablar de 'partes interesadas' o *stakeholders*

Calidad en el software

- Aspectos importantes sobre calidad en software:
- Los **requisitos del software** son la base de las medidas de calidad
  - La falta de concordancia con los requisitos es una falta de calidad
  - El aseguramiento de la calidad se basa en la implantación de metodologías y normativas técnicas y de gestión
    - La gestión y el control. Un sistema de gestión de la calidad con los mismos requisitos de normas como la ISO 9001
  - La norma ISO 9000:2005 define el concepto 'requirement' en inglés, y su significado se corresponde con 'requisito'
    - Requirement ↔ requisito, requerimiento ↔ request
  - Estándares o metodologías → conjunto de criterios de desarrollo
  - Si no se sigue ninguna metodología siempre habrá falta de calidad

Calidad en el software

- La calidad debe perdurar en el tiempo
  - El día después de desarrollar el software importa incluso más que cuando se entrega
  - Un buen mantenimiento también implica calidad
- Cumplimiento de aspectos legales
  - Privacidad y protección de datos personales, propiedad intelectual, comercio electrónico, etc.
- La calidad en el software implica un fuerte componente técnico en la propia gestión interna
  - Separación de entornos de desarrollo, test y producción, subcontratación de servicios a terceros, y control hacia ellos

Calidad en el tratamiento de la información

- La información es un pilar fundamental en la empresa
  - Tanto si la empresa es tecnológica como si no
- Las nuevas herramientas TIC deben aplicarse según objetivos empresariales con la mayor seguridad, garantizando:
  - Confidencialidad: sólo quienes estén autorizados pueden acceder a la información
  - Integridad: la información es fiable y exacta
  - Disponibilidad: los usuarios autorizados tienen el acceso debido a la información
- Además del cumplimiento de la Ley, la calidad en TIC repercute directamente en la rentabilidad y el prestigio de la empresa

Entidades de certificación

- Las entidades de certificación están reconocidas legalmente con distintos ámbitos (nacional, europeo, mundial)
- Tienen atribuciones para certificar el cumplimiento de los estándares a las empresas (p. ej: una norma ISO), y pueden ser entidades públicas o privadas
- El proceso de certificación suele incluir una auditoría y una emisión de informes, además de suponer un coste económico
  - La validez de los certificados es limitada en el tiempo y su renovación conlleva más auditorías y pagos
- Las certificaciones proporcionan a las organizaciones un planteamiento estructurado para cumplir determinados objetivos (según la norma a certificar)
  - Es un reto, pero también es una oportunidad que tienen las empresas para generar más clientes y abrirse a nuevos mercados

Aenor

- La Asociación Española de Normalización y Certificación (Aenor) es una entidad privada dedicada al desarrollo de la normalización y la certificación (N+C) en todos los sectores industriales y de servicios
- Fue creada por Orden del Ministerio de Industria y Energía, de 26 de febrero de 1986, de acuerdo con el Real Decreto 1614/1985 y reconocida como organismo de normalización y para actuar como entidad de certificación por el Real Decreto 2200/1995, en desarrollo de la Ley 21/1992, de Industria
- Las funciones de AENOR son:
  - Elaborar normas técnicas españolas (UNE) con la participación abierta a todas las partes interesadas y representar a España en los distintos organismos de normalización regionales e internacionales
  - Certificar productos, servicios y empresas

IqNet

- Entidad certificadora internacional, que agrupa a más de 30 de los principales organismos certificadores de diferentes países (Aenor en España)
- Los certificados IQNet tienen validez mundial
  - Los de Aenor sólo en España
  - Pero Aenor (como miembro de IqNet) también expide el internacional

IQNet®

THE INTERNATIONAL CERTIFICATION NETWORK

CERTIFICATE

IQNet and
AENOR
hereby certify that the organization

Nombre de la empresa

for the following field of activities

Amicable and judicial debt collection,

has implemented and maintains a

Quality Management System

which fulfills the requirements of the following standard

ISO 9001:2000

Issued on: 2007-07-09 Validity date: 2010-07-09

Registration Number:

IQNet AENOR

René Wasmer
President of IQNet

Ramón NAZ
General Manager of AENOR

IQNet Partners*:
AENOR Spain AFAQ AFNOR France AIB-Vincotte International Belgium ANCE Mexico APCER Portugal CISQ Italy CQC China CQM China CQS Czech Republic Cro Cert Croatia DQS Germany DS Denmark ELOT Greece FCAV Brazil FONDONORMA Venezuela HKQAA China ICONTEC Colombia IMNC Mexico IRAM Argentina JQA Japan KFQ Korea MSZT Hungary Nemko AS Norway NSAI Ireland PCBC Poland PSB Certification Singapore QMI Canada Quality Austria Austria RR Russia SAI Global Australia Inspecta Certification Finland SII Israel SIQ Slovenia SQS Switzerland SRAC Romania TEST St Petersburg Russia YUQS Serbia and Montenegro
IQNet is represented in the USA by: AFAQ AFNOR, AIB-Vincotte International, CISQ, DQS, NSAI, QMI and SAI Global
* The list of IQNet partners is valid at the time of issue of this certificate. Updated information is available under www.iqnet-certification.com

ISO

- Organización Internacional de Normalización (del griego *isos*, que significa *igual*), creada en 1947 tras la Segunda Guerra Mundial
- Promueve el desarrollo de normas internacionales de fabricación de productos y servicios, comercio y comunicación para todas las ramas industriales (a excepción de la eléctrica y la electrónica)
- Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones (públicas o privadas) a nivel internacional

ISO

- La ISO es una red de los institutos de normas nacionales de 161 países
  - Con una Secretaría Central en Ginebra (Suiza) que coordina el sistema
  - Está compuesta por delegaciones gubernamentales y no gubernamentales subdivididos en una serie de subcomités
- Las normas desarrolladas por ISO son voluntarias
  - ISO es un organismo no gubernamental y no depende de ningún otro organismo internacional
  - No tiene autoridad para imponer sus normas a ningún país
  - El contenido de los estándares está protegido por derechos de copyright y para acceder a ellos el usuario normal debe comprar cada documento

IEC

- Comisión Electrotécnica Internacional
  - IEC: International Electrotechnical Commission
- Es una organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas
  - Son campos donde no interviene la ISO
- Muchas normas se desarrollan conjuntamente con la ISO
  - Normas ISO/IEC
  - Esto es así porque afectan a varias disciplinas simultáneamente

Principales normas de calidad para desarrollo de software

- **ISO 9001** aplicada al software
  - Aplicada a cualquier proceso productivo de la organización
    - No sólo sobre el desarrollo, también sobre identificación de requisitos, mantenimiento…
  - Está muy extendida (casi cualquier empresa puede conseguirlo)
- ISO/IEC 9003 (Ingeniería del software)
  - Guía de aplicación de la ISO 9001:2000 al software (no es certificable)
  - Guía de buenas prácticas para definir con más detalle los conceptos de software sobre los procesos de la organización
- ISO/IEC 9126
  - Definición de atributos clave de calidad para el software

Principales normas de calidad para desarrollo de software

- ISO/IEC 12207 (*Information Technology / Software Life Cycle Processes)*
  - Estándar para los procesos de ciclo de vida del software de la organización
  - Es la base para ISO 15504-SPICE
- **ISO/IEC 15504** (SPICE - *Software Process Improvement And Assurance Standards Capability Determination*)
  - Un conjunto de 7 normas para establecer y mejorar la capacidad y madurez de los procesos de las organizaciones
  - Proporciona los principios para realizar una **evaluación de la calidad de los procesos**

Principales normas de calidad para desarrollo de software

- **ISO/IEC 25000** (Square). Evaluación de la calidad del software
  - Evolución de ISO/IEC 9126**.** *Software engineering – Product quality*
  - Define las características de calidad del **producto de software**, las métricas internas y externas, y la calidad en el uso
- **Capability Maturity Model Integration (CMMI)**
  - Evaluación por niveles de capacidad y de madurez
  - La norma provee una guía para implementar una estrategia de calidad y mejorar los procesos de una organización que se dedica al desarrollo y/o mantenimiento de software
  - Dispone de un esquema de certificación creado sobre organismos privados (nada que ver con normas ISO)
  - Se ha convertido mundialmente en un requisito para acceder a la exportación de servicios de software

Principales normas de calidad para empresas TIC

- **ISO/IEC 20000**
  - La familia de normas 20000 establece un modelo de calidad y de evaluación de los productos
    - Puede ser software o cualquier producto fabricado/creado
- **ISO/IEC 27000**
  - Conjunto de normas relacionadas con la **gestión de la seguridad de la información**
  - Muy de moda últimamente con los problemas de protección de datos en las empresas y las nuevas legislaciones sobre acceso a la información

El proceso de certificación

- Adecuar el modo de trabajo y la estructura organizativa de la empresa a una norma aporta una serie de beneficios:
  - Prestigio reconocido de la compañía
  - Mejora en la productividad y la eficiencia
  - Ahorro y disminución de gastos (a medio y largo plazo)
  - Definición de roles y responsabilidades más precisos
  - Mejora de la fiabilidad de sus operaciones internas para satisfacer las necesidades de los clientes y también para aumentar su rendimiento global
  - Evaluación periódica de los procesos de gestión de servicios TI, lo que ayuda a mantener y mejorar la eficacia
  - Estandarización de la infraestructura y alineamiento con los programas de calidad
- Por tanto, la certificación no debería ser un fin en sí misma
  - No hay que buscar tener el certificado colgado en la pared como un título más

El proceso de certificación

- No todas las empresas tienen que certificarse en todo lo posible
  - Hay que seleccionar la estandarización de lo más importante y lo que más proyección tiene hacia el cliente
  - No olvidemos que la certificación se hace de cara al exterior (prestigio)
  - Una empresa siempre puede asimilar una parte de las normas y no buscar el obtener los certificados (por el coste que lleva)
    - La normas también sirven de manual de organización para la empresa
- Una vez se toma la decisión de aspirar a una certificación es necesario cubrir una serie de actividades
  - Estarán involucrados tanto la empresa solicitante como la entidad de certificación
  - Cada cierto tiempo habrá que renovar el certificado

El proceso de certificación

- Los pasos habituales para la certificación son:
  - Determinar el alcance de la certificación
  - Solicitud de certificación a la entidad correspondiente (ej: Aenor)
  - Análisis de documentación (ej: una norma ISO)
  - Visita previa
  - Auditoría inicial (antes se puede hacer una a nivel interno)
  - Evaluación y decisión
  - Concesión del certificado
  - Auditoría de seguimiento
  - Auditoría de renovación (anual o cada x años, normalmente 3)
- En varias etapas hay que hacer los pagos correspondientes

El proceso de certificación

- El coste de la certificación es diverso
  - El pago a la entidad propietaria de la norma (ej: ISO) a través de una comercializadora: lo que se compran son los documentos
  - El pago a la entidad certificadora (ej: Aenor) por los servicios de auditoría y certificación
    - Depende del tiempo dedicado, de la cantidad de trabajo a realizar y del volumen de la estructura organizativa de la empresa
    - Suelen ser unos miles de euros
  - El coste en personas/hora o personas/mes
    - Tanto de la entidad certificadora como de la propia empresa (deben dedicarse a esta tarea y dejar de producir durante ese tiempo)
    - Este es el mayor coste, y el más difícil de calcular y justificar ante la junta directiva

Normas y certificados de calidad para desarrollo de software

ISO/IEC 9126

- **ISO/IEC 9126**
  - El estándar ISO 9126 ha sido desarrollado en un intento de identificar los atributos clave de calidad para el software
  - Funcionalidad**:** el grado en que el software satisface las necesidades indicadas por:
    - Idoneidad
    - Corrección
    - Interoperatividad
    - Conformidad
    - Seguridad
  - Confiabilidad: cantidad de tiempo que el software está disponible para su uso
    - Madurez
    - Tolerancia a fallos
    - Facilidad de recuperación

ISO/IEC 9126

- **ISO/IEC 9126**
  - Usabilidad: grado en que el software es fácil de usar
    - Facilidad de comprensión
    - Facilidad de aprendizaje
    - Operatividad
  - Eficiencia: grado en que el software hace óptimo el uso de los recursos del sistema
    - Tiempo de uso
    - Recursos utilizados

ISO/IEC 9126

- **ISO/IEC 9126**
  - Facilidad de mantenimiento: la facilidad con que una modificación puede ser realizada
    - Facilidad de análisis
    - Facilidad de cambio
    - Estabilidad
    - Facilidad de prueba
  - Portabilidad: la facilidad con que el software puede ser llevado de un entorno a otro
    - Facilidad de instalación
    - Facilidad de ajuste
    - Facilidad de adaptación al cambio

ISO/IEC 15504 (SPICE)

- **ISO/IEC 15504**
  - También conocido como ***Software Process Improvement Capability Determination*** **(SPICE)**
  - Determinación de la Capacidad de Mejora del Proceso de Software
- Es un modelo para la mejora, evaluación de los procesos de desarrollo, mantenimiento de sistemas de información y productos de software
- Esta norma evalúa la calidad software por *niveles de madurez* y la mejora de procesos ya existentes en la empresa
  - Se parece mucho a CMMI (se verá más adelante)

ISO/IEC 15504 (SPICE)

- En el marco europeo y español Spice es la opción que está más evolucionanda en la pyme
- Es un modelo que se puede realizar por pasos y adaptarlo a todo tipo de empresas
  - Parte específica para pequeñas empresas "mini Spice“
- La norma está en continuo desarrollo
- La implantación y evaluación externa para la *certificación* se puede realizar por etapas, de tal manera que en años posteriores se va aumentando su alcance
  - Se certifica sobre ISO/IEC 15504-2 y con los requisitos de niveles de madurez y clases de evaluaciones según ISO/IEC TR 15504-7:2008

CMMI

- Capability Maturity Model Integration (**CMMI**)
  - Integración de modelos de madurez de capacidades
  - Es una norma dirigida a grandes empresas o que requieren requisitos de calidad muy altos (es costosa)
- No es ISO aunque su certificación otorga el prestigio necesario
  - El equivalente ISO es la 15504 (SPICE)
- Su certificación consiste en verificar y puntuar en qué nivel de madurez se encuentra la organización (por el instituto CMMI)
- Está especialmente indicada para empresas cuyos procesos de software se realizan en países fuera de sus oficinas centrales o en organizaciones que ofrecen el off-shoring/outsourcing del desarrollo de software

CMMI

- Evaluación por niveles de capacidad y de madurez
  - Tanto CMMI como ISO/IEC 15504 (SPICE) usan este modelo de evaluación
- Hay dos maneras de hacer las evaluaciones
  - Por niveles de madurez, donde se obtiene una puntuación cuyo alcance es la organización (departamento, o proyecto, etc.)
  - Por niveles de capacidad, o de manera continua, donde la organización obtiene puntuación para un proceso concreto (por ejemplo para la gestión de requisitos, o la planificación de proyectos, gestión de la configuración, etc.)
- El nivel más alto es 5
  - Sólo el ~7% de las empresas en el mundo
  - Sólo el ~4% en España (ej: Indra)

ISO/IEC 25000 (SQUARE)

- ISO/IEC 25000 (**Square**)
  - *System and Software Quality Requirements and Evaluation:* SQuaRE
- Familia de normas que tiene por objetivo la creación de un marco de trabajo común para evaluar la calidad del producto software
- La familia ISO/IEC 25000 es el resultado de la evolución de otras normas anteriores
  - ISO/IEC 9126, que describe las particularidades de un modelo de calidad del producto software
  - ISO/IEC 14598, que abordaba el proceso de evaluación de productos software

ISO/IEC 25000 (SQUARE)

- ISO/IEC 25000 se encuentra compuesta por cinco divisiones

ISO/IEC 25000 (SQUARE)

- **ISO/IEC 2500n – División de Gestión de Calidad**
  - Definen todos los modelos, términos y definiciones comunes referenciados por todas las otras normas de la familia 25000
    - ISO/IEC 25000 - *Guide to SQuaRE*: la terminología de la familia, un resumen de las partes, los usuarios previstos y las partes asociadas, así como los modelos de referencia
    - ISO/IEC 25001 - *Planning and Management*: requisitos y orientaciones para gestionar la evaluación y especificación de los requisitos del producto software
- **ISO/IEC 2501n – División de Modelo de Calidad**
  - Modelos de calidad detallados: calidad interna, externa y en uso del producto
    - ISO/IEC 25010 - *System and software quality models*: describe el modelo de calidad para el producto software y para la calidad en uso
    - ISO/IEC 25012 - *Data Quality model*: define un modelo general para la calidad de los datos, aplicable a aquellos datos que se encuentran almacenados de manera estructurada y forman parte de un Sistema de Información

ISO/IEC 25000 (SQUARE)

- **ISO/IEC 2502n – División de Medición de Calidad**
  - Modelo de referencia de la medición de la calidad del producto
    - ISO/IEC 25020 - *Measurement reference model and guide*: presenta una explicación introductoria y un modelo de referencia común a los elementos de medición de la calidad
    - ISO/IEC 25021 - *Quality measure elements*: define y especifica un conjunto recomendado de métricas base y derivadas que puedan ser usadas a lo largo de todo el ciclo de vida del desarrollo software
    - ISO/IEC 25022 - *Measurement of quality in use*: define específicamente las métricas para realizar la medición de la calidad en uso del producto.
    - ISO/IEC 25023 - *Measurement of system and software product quality*: define específicamente las métricas para realizar la medición de la calidad de productos y sistemas software
    - ISO/IEC 25024 - *Measurement of data quality*: define específicamente las métricas para realizar la medición de la calidad de datos

ISO/IEC 25000 (SQUARE)

- **ISO/IEC 2503n – División de Requisitos de Calidad**
  - Ayudan a especificar los requisitos de calidad del producto software a desarrollar o como entrada del proceso de evaluación
- **ISO/IEC 2504n – División de Evaluación de Calidad**
  - Normas que proporcionan requisitos, recomendaciones y guías para llevar a cabo el proceso de evaluación del producto software
    - ISO/IEC 25040 - *Evaluation reference model and guide*: propone un modelo de referencia general para la evaluación, que considera las entradas al proceso de evaluación, las restricciones y los recursos necesarios para obtener las correspondientes salidas
    - ISO/IEC 25041 - *Evaluation guide for developers, acquirers and independent evaluators*: describe los requisitos y recomendaciones para la implementación práctica de la evaluación del producto software desde el punto de vista de los desarrolladores, de los adquirentes y de los evaluadores independientes
    - ISO/IEC 25042 - *Evaluation modules*: define lo que la Norma considera un módulo de evaluación y la documentación, estructura y contenido que se debe utilizar a la hora de definir uno de estos módulos
    - ISO/IEC 25045 - *Evaluation module for recoverability*: define un módulo para la evaluación de la subcaracterística Recuperabilidad

Normas y certificados de calidad TIC

ISO 9000

- La serie **ISO 9000** es una gama de normas con el objetivo de **ordenar la gestión de la empresa y dotarla de calidad en sus servicios**
- Ha ganado un gran reconocimiento y aceptación internacional como certificación de calidad en los procesos productivos de las empresas (a todos los niveles)
- La familia de normas se divide en dos grupos principales:
  - Especificaciones de requisitos para sistemas de calidad
    - ISO 9001, 9002, 9003
  - Guía para ayudar en la interpretación y puesta en práctica del sistema de calidad
    - ISO 9000-2, ISO 9004-1

ISO 9000

- Objetivos
  - Proporcionar elementos para que una organización pueda lograr la calidad del producto o servicio, a la vez que mantenerla en el tiempo
    - Permite a la empresa reducir costos de calidad, aumentar la productividad, y destacarse o sobresalir frente a la competencia
  - Proporcionar a los clientes o usuarios la seguridad de que el producto o los servicios tienen la calidad deseada, concertada, pactada o contratada
  - Proporcionar a la dirección de la empresa la seguridad de que se obtiene la calidad deseada
  - Establecer las directrices mediante las cuales la organización puede seleccionar y utilizar las normas

ISO 9000

- ISO-9001: especifica los requisitos que debe cumplir un sistema de calidad, aplicables cuando un contrato entre dos partes exige que se demuestre la capacidad de un proveedor en el diseño, desarrollo, producción, instalación y servicio posventa del producto suministrado
- ISO-9002: busca la capacidad de un proveedor en la producción, instalación y servicio posventa del producto
- ISO-9003: se centra en la capacidad de un proveedor en la inspección, y ensayos finales del producto suministrado
- ISO-9004: Aquí el elemento clave es el conjunto de evaluaciones internas de liderazgo, estrategia, recursos y procesos

ISO/IEC 20000

- La norma **ISO/IEC 20000** se concentra en la **gestión de problemas de tecnologías de la información** mediante el uso de un planteamiento de servicio de asistencia
  - Fue publicada en diciembre de 2005
- Con esta norma se **clasifican las contingencias**, lo que ayuda a identificar problemas continuados o interrelacionados
- También se considera la capacidad del sistema, los niveles de gestión necesarios cuando éste cambia, la asignación de presupuestos financieros, y la supervisión del control y distribución del software

ISO/IEC 20000

- Es la primera norma en el mundo específicamente dirigida a la gestión de los servicios de TI (Tecnologías de la Información)
- Fue desarrollada en respuesta a la necesidad de establecer procesos y procedimientos para minimizar los riesgos en los negocios provenientes de un colapso técnico del sistema de TI de las organizaciones
- Describe un conjunto integrado de procesos que permiten prestar de forma eficaz servicios de TI a las organizaciones y a sus clientes
  - Está orientada al desarrollo de la certificación en ITSM (IT Service Management)

ISO/IEC 20000

- La **norma ISO/IEC 20000** está formada por cinco partes
- **ISO 20000-1**: Especificaciones
  - Establece los requisitos que necesitan las empresas para diseñar, implementar y mantener la gestión de servicios TI
  - Plantea un mapa de procesos que permite ofrecer servicios de TI con una calidad aceptable
- **ISO 20000-2**: Código de buenas prácticas
  - Describe las mejoras prácticas adoptadas por la industria en relación con los procesos de gestión del servicio TI, que permite cubrir las necesidades de negocio del cliente, con los recursos acordados, así como asumir un riesgo entendido y aceptable

ISO/IEC 20000

- **ISO 20000-3**: Guía sobre definición del alcance y aplicabilidad de la ISO 20000-1
  - Proporciona orientación sobre la definición del alcance, aplicabilidad y la demostración de la conformidad con los proveedores de servicios orientados a satisfacer los requisitos de la norma ISO 20000-1
  - También contempla a los proveedores de servicios que están planeando mejoras con la intención de utilizar la norma como un objetivo de negocio
- **ISO 20000-4**: Modelo de referencia de procesos (un informe técnico)
  - Describe de manera abstracta un modelo de procesos para la gestión de los servicios IT en base a la ISO 20000-1
  - Para cada proceso se describe su propósito y los resultados (outcomes)
  - Sirve para cumplir con los requisitos de ISO 20000-1 y poder evaluarse con la 15504
- **ISO 20000-5**: Modelo (ejemplo) de plan de implementación de ISO/IEC 20000-1

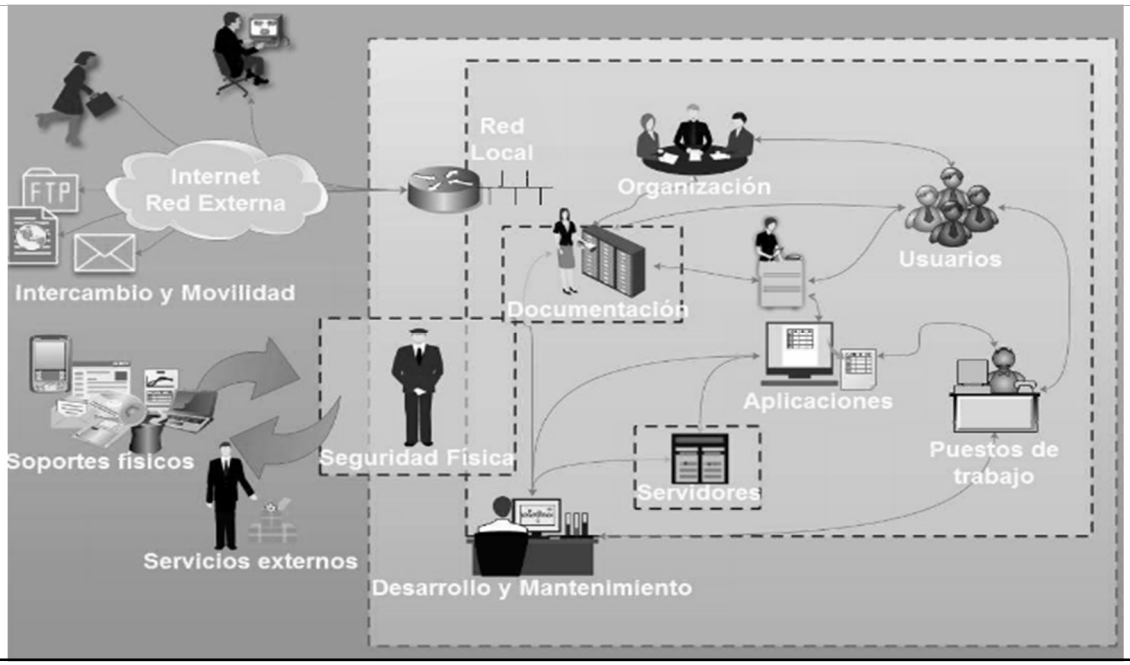
ISO/IEC 20000

- El objetivo de conseguir la **certificación ISO 20000**, no es otro que el de demostrar que una organización de TI tiene la capacidad suficiente de satisfacer las necesidades y expectativas de sus clientes
- La **certificación ISO 20000** puede ser usada por los siguientes motivos:
  - Negocios que requieran de un enfoque consistente por parte de todos sus proveedores de servicios
  - Necesidad de los proveedores de servicio de evaluar y comparar su Gestión de Servicios TI
  - Necesidad de demostrar la capacidad de una organización para proveer servicios que cumplan con los requerimientos de los usuarios
  - Búsqueda de mejora de servicios por medio de una aplicación efectiva de procesos para monitorizar y mejorar la calidad de los servicios

ISO/IEC 27000

- La serie **ISO 27000** está dedicada a la **gestión de la seguridad de la información**
  - De manera similar a la serie ISO 9000
  - Una empresa que tenga establecida la ISO 27000 garantiza, tanto de manera interna como al resto de las empresas, que los riesgos de la seguridad de la información son controlados por la organización de una forma eficiente
  - Se define el **SGSI** (Sistema de Gestión de Seguridad de la Información)
- Objetivos:
  - Preservar la confidencialidad de los datos de la empresa
  - Conservar la integridad de estos datos
  - Hacer que la información protegida se encuentre disponible

ISO/IEC 27000



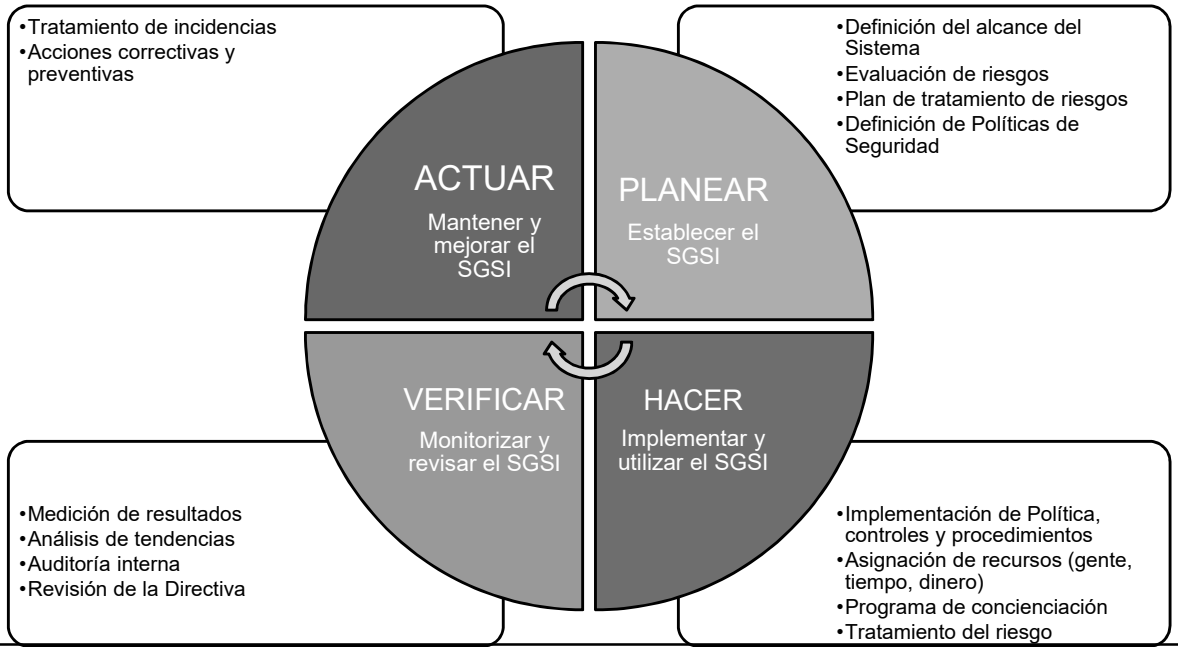
ISO/IEC 27000

- ISO/IEC 27000
  - Define el vocabulario, términos y conceptos empleados en la familia 27000
- ISO/IEC 27001
  - Define los requisitos para implantar un SGSI certificable conforme a ISO 27000
  - Define un SGSI, su gestión y las responsabilidades de los participantes
  - Sigue un modelo **PDCA** (Plan-Do-Check-Act)
    - Ciclo Deming: Planificar-Hacer-Verificar-Actuar
  - Tiene como punto clave la gestión de riesgos unida con la mejora continua
- ISO/IEC 27002
  - Define las buenas prácticas para la gestión de la seguridad
  - Medidas a tomar para asegurar los sistemas de información de una organización
  - Identifica los objetivos de control y los controles recomendados a implantar
  - Antes ISO 17799, basado en estándar BS 7799

ISO/IEC 27000 : 27001

- Plan-Do-Check-Act (PDCA o **ciclo de Deming**) para todos los procesos de seguridad de la información en la organización
  - Fase de Planificación (Plan)
    - Establecer la política, objetivos, procesos y procedimientos relativos a la gestión del riesgo y mejorar la seguridad de la información de la organización
  - Fase de Ejecución (Do)
    - Implementar y gestionar el SGSI de acuerdo a su política, controles, procesos y procedimientos
  - Fase de Seguimiento (Check)
    - Medir y revisar las prestaciones de los procesos del SGSI
  - Fase de Mejora (Act)
    - Adoptar acciones correctivas y preventivas basadas en auditorías y revisiones internas o en otra información relevante para alcanzar la mejora continua del SGSI

ISO/IEC 27000 : 27001

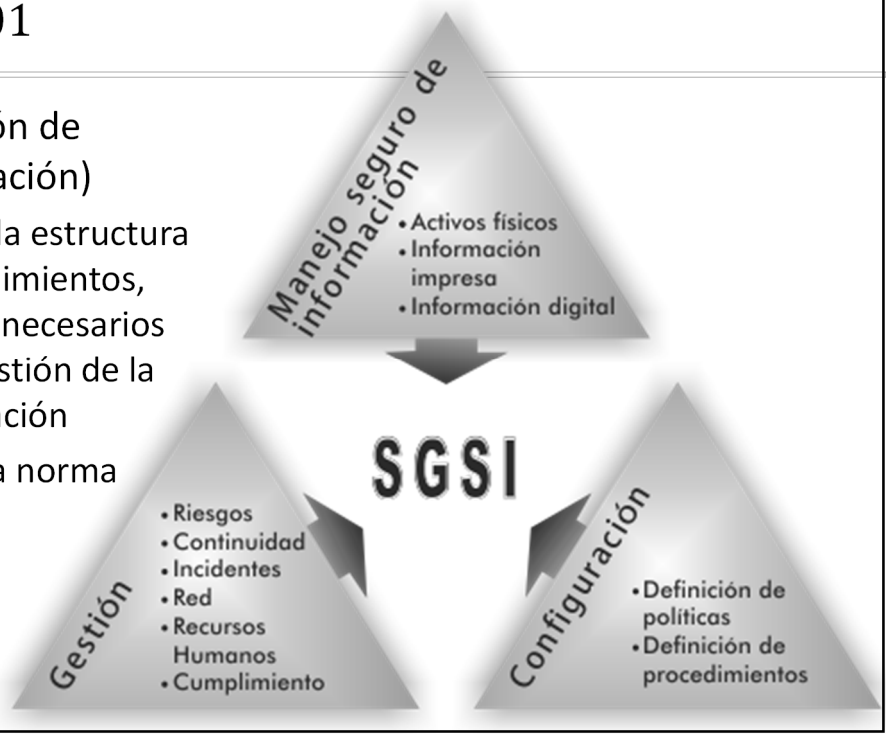


ISO/IEC 27000 : 27001

- Seguridad de la información
  - Se define la seguridad de la información como el logro, gestión y mantenimiento de tres características elementales
    - Confidencialidad: La información sólo debe ser vista por aquellos que tienen permiso para ello
    - Integridad: La información podrá ser modificada solo por aquellos con derecho a cambiarla
    - Disponibilidad: La información deberá estar disponible en el momento en que los usuarios autorizados requieren acceder a ella

ISO/IEC 27000 : 27001

- **SGSI** (Sistema de Gestión de Seguridad de la Información)
  - Comprende la política, la estructura organizativa, los procedimientos, procesos y los recursos necesarios para implementar la gestión de la seguridad de la información
  - Es el punto central de la norma 27000



ISO/IEC 27000 : 27002

- ISO 27002: Conjunto de recomendaciones sobre qué medidas tomar en la empresa para asegurar los Sistemas de Información
  - Política de seguridad
  - Aspectos organizativos para la seguridad
  - Clasificación y control de activos
  - Seguridad ligada al personal
  - Seguridad física y del entorno
  - Gestión de comunicaciones y operaciones
  - Control de accesos
  - Desarrollo y mantenimiento de sistemas
  - Gestión de incidentes de seguridad de la información
  - Gestión de continuidad de negocio
  - Conformidad

ISO/IEC 27000 – Diferencias entre 27001 y 27002

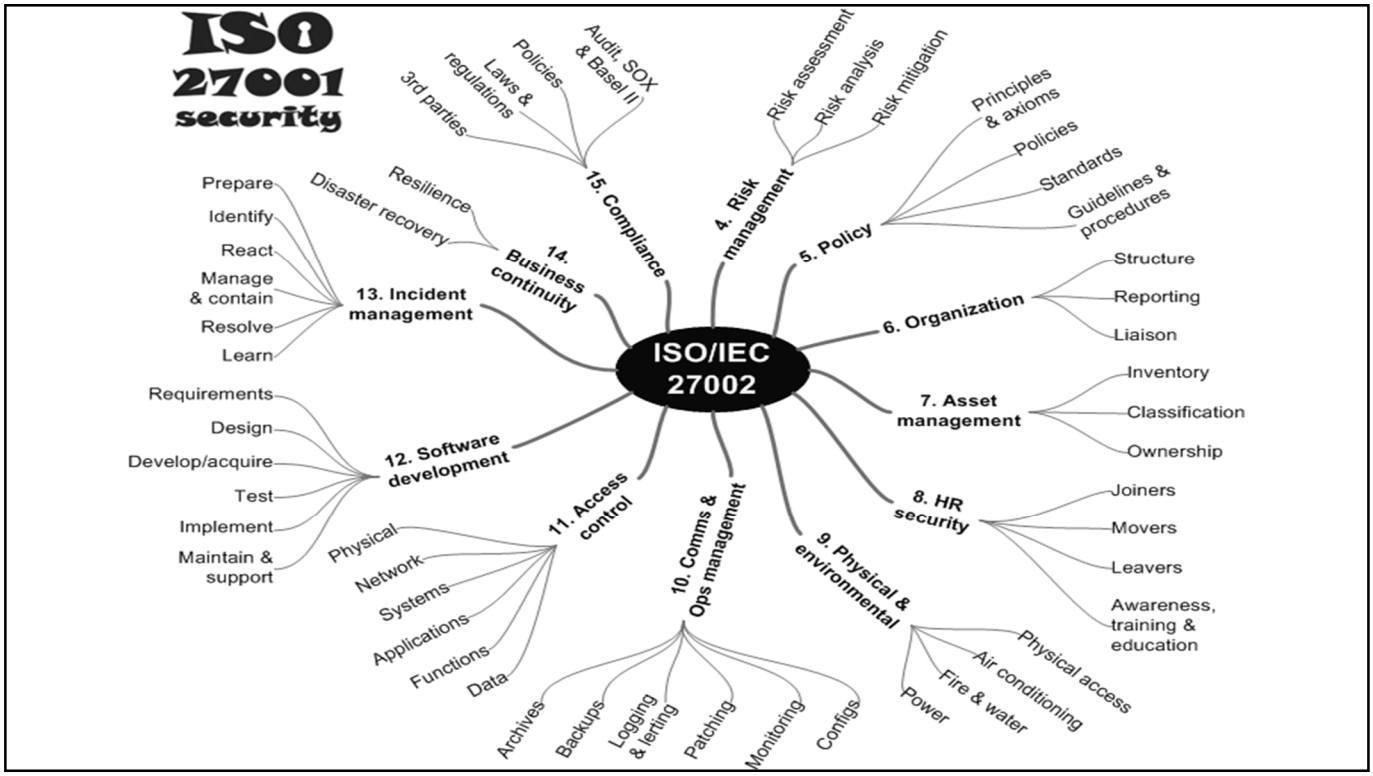
- ISO 27001 define el SGSI, ISO 27002 define cómo implementarlo
  - La ISO 27002 es mucho más detallada y mucho más precisa
  - Los controles de la norma ISO 27002 tienen la misma denominación que los indicados en el Anexo A de la ISO 27001, la diferencia se presenta en el nivel de detalle
- No es posible obtener la certificación ISO 27002 porque no es una norma de gestión
  - La certificación en ISO 27001 sí es posible

ISO/IEC 27000 – Diferencias entre 27001 y 27002

- ISO 27001 establece que el sistema de gestión implica:
  - La seguridad de la información debe ser planificada, implementada, supervisada, revisada y mejorada
  - La gestión tiene sus responsabilidades específicas
  - Se deben establecer, medir y revisar objetivos
  - Se deben realizar auditorías internas, etc.
  - Todo esto no está establecido en la ISO 27002
- Se usa la ISO 27001 para crear la estructura de la seguridad de la información en la organización
- Se usa la ISO 27002 para implementar los controles de seguridad

ISO/IEC 27000 – Diferencias entre 27001 y 27002

- Lo ideal es utilizar la ISO 27001 y la ISO 27002 en conjunto
- Sin la descripción proporcionada por la ISO 27002, los controles definidos en el Anexo A de la ISO 27001 no se podrían implementar
- Sin el marco de gestión de la ISO 27001, la ISO 27002 es un esfuerzo aislado por la seguridad de la información, sin la aceptación de la alta dirección y sin efectos reales sobre la organización



ISO/IEC 27000

- Fases de la auditoría del Sistema de gestión de la seguridad de la información (SGSI)