**UNIDAD V**
**NORMATIVIDAD DE LA FUNCIÓN INFORMÁTICA**

OBJETIVO: El alumno identificará y aplicará los diversos tipos de estándares propios a un centro de informática.

Introducción

Las normas son especificaciones técnicas, de carácter voluntario, consensuadas, elaboradas con la participación de las partes interesadas (fabricantes, usuarios y consumidores, laboratorios, administración, centros de investigación) y aprobadas por un organismo reconocido.

Estas normas tienen el carácter de acuerdos documentados y contienen las especificaciones técnicas o criterios precisos para ser usados consistentemente como reglas, guías, o definiciones de características, asegurando de esta forma que los materiales, productos, procesos y servicios son apropiados para lograr el fin para el que se concibieron.

La normalización contribuye a simplificar y a incrementar la fiabilidad y eficiencia de los bienes y servicios que utilizamos, así como a mejorar el bienestar de la sociedad y redunda en el beneficio común.

Las normas son, por tanto, documentos de aplicación voluntaria, elaborados por las partes interesadas, por consenso y aprobados por un organismo reconocido.

En el ámbito internacional ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) tienen por objeto favorecer el desarrollo de la normalización en el mundo, con vistas a facilitar los intercambios comerciales y las prestaciones de servicios entre los distintos países. Los trabajos desarrollados por ISO cubren prácticamente todos los sectores de la técnica, con excepción del campo eléctrico y electrotécnico, cuya responsabilidad recae en IEC. Los miembros de ISO o IEC son los organismos que representan la normalización de un país. Tan sólo un organismo de cada país puede ser miembro de estas organizaciones. La participación en los comités técnicos de ISO/IEC puede ser como miembro bien “P” (participante) o bien “O” (observador).

Los órganos de trabajo técnicos de ISO son los siguientes:

- Comités Técnicos (CT): su función principal es el desarrollo de las normas internacionales y su revisión, en caso de que fuera necesario. Cada CT puede, si así lo cree conveniente debido a la amplitud de su campo de actuación, establecer subcomités y/o bien grupos de trabajo para cubrir temas específicos.

- Subcomités (SC): tienen las mismas atribuciones que el CT y autonomía para realizar sus trabajos, con la única obligación de mantener informado al CT de sus actividades.

- Grupos de Trabajo (GT): se crean para trabajos específicos emprendidos por el comité/subcomité.

Los documentos elaborados por ISO/IEC son, principalmente, de dos tipos:

- ✓ Norma internacional (ISO/IEC): norma elaborada por los miembros participantes en un comité técnico, subcomité o grupo de trabajo y aprobada por votación entre todos los participantes.

- ✓ Informe Técnico (TR): documento técnico elaborado para informar sobre los progresos técnicos de un tema determinado, dar recomendaciones sobre la ejecución de un trabajo y facilitar información y datos distintos a los que generalmente están contenidos en una norma.

En el ámbito europeo CEN (Comité Europeo de Normalización) contribuye a los objetivos de la Unión Europea y del espacio económico europeo con estándares técnicos de uso voluntario para facilitar el intercambio de bienes y servicios, eliminar barreras técnicas, fomentar la competitividad de la industria europea y ayudar a la creación del mercado interior europeo.

Así, CEN produce normas en materias tales como el comercio libre, la seguridad de trabajadores y consumidores, la seguridad e interoperabilidad de las redes, la protección del medio ambiente, la explotación de los programas de investigación y desarrollo y la administración pública.

CEN emite principalmente:

- Normas europeas (EN, European Standards).
- Especificaciones técnicas (TS, Technical Specifications).
- Informes técnicos (TR, Technical Reports).

Una norma europea (EN) conlleva la obligación de ser adoptada como una norma nacional idéntica y de anular las normas nacionales divergentes. Cuando se elaboran a solicitud de la Comisión Europea y/o bien la Asociación Europea de Libre Comercio se conoce como normas europeas mandatadas. Puede tratarse de normas que apoyan directivas comunitarias o políticas comunitarias en diversas cuestiones, como políticas industriales o de seguridad de los consumidores, por ejemplo.

Finalmente, una norma armonizada es una norma mandatada que ofrece soluciones técnicas necesarias para dar presunción de conformidad con los requisitos esenciales de una o varias directivas, y sus referencias se han de publicar en el Diario Oficial de la Unión Europea.

En 1997 se creó CEN/ISSS (Comité Europeen de Normalisation / Information Society Standardization System) para centralizar las actividades de normalización europea en materia de tecnologías de la información y las comunicaciones. En particular, los talleres de CEN/ISSS producen los CEN Workshop Agreements (CWA).

En el ámbito nacional AENOR, la Asociación Española de Normalización y Certificación, asumió la responsabilidad internacional en ISO en 1987, en IEC en 1995 y es, por tanto, el comité miembro que representa los intereses españoles en el campo de la normalización ante dichas organizaciones y quien distribuye los productos de ISO/IEC, CEN/CENELEC, así como las normas UNE.

De la normalización en materia de seguridad de las tecnologías de la información se ocupan respectivamente, en el ámbito internacional de ISO/IEC el subcomité ISO/IEC JTC 1/SC 27, en el ámbito europeo de CEN el órgano CEN/ISSS, en el ámbito nacional de AENOR el subcomité espejo AEN/CTN 71/SC 27.

El derecho es aplicable a todos los individuos, también la normatividad aplicada al hardware, es fundamentalmente necesaria para tener conocimiento y respeto al equipo de cómputo, es fundamental para no cometer errores o quizás hasta delitos informáticos como hackear o crackear, o falsificar documentos, es esencialmente difícil no encontrar en la actualidad esta problemática mundial que afecta en términos de integridad y laborales.

Ejemplos de normativas aplicadas al equipo:

- Artículo 2: De la responsabilidad

De la Ley aplicable, se determina su adquisición:

I.- Por cada equipo de cómputo, habrá un servidor público responsable, quién deberá observar las disposiciones de esta normatividad, auxiliado por el administrador de la unidad informática, quién a su vez es responsable directo, de todos los bienes informáticos que por función le corresponda administrar.

Tanto los responsables como los administradores de unidades informáticas, deberán verificar los equipos de cómputo con objeto de constatar el cumplimiento escrupuloso de la normatividad establecida de acuerdo a la legislación aplicable.

- Artículo 3: Del respaldo, ambiente y limpieza

El equipo de cómputo deberá mantenerse en un sitio apropiado, iluminado, ventilado, limpio y libre de polvo, así mismo, los responsables a través de los administradores de la unidad informática, deberán solicitar, a la Dirección General de Modernización y Sistemas su inclusión en el programa permanente de mantenimiento preventivo.

III.- Queda estrictamente prohibido el almacenamiento de archivos que contengan música, pornografía, videos, imágenes y de cualquier otro tipo que no estén relacionados con la actividad ó función, para la cual se destinó el equipo de cómputo.

- Artículo 6: De los servicios institucionales

Es responsabilidad de los administradores de unidades informáticas, instalar ó, en su caso, solicitar la instalación del software correspondiente a los servicios institucionales que le hayan sido autorizados al equipo de cómputo de su área de competencia a fin de mantenerlos vigentes.

- Artículo 8: De las adquisiciones de equipo de cómputo y suministros

I.- La Dirección General de Modernización y Sistemas analizará y presentará el dictamen técnico de las requisiciones de equipo, software y suministros para equipo de cómputo a fin de asegurar que alcancen la mayor utilidad y compatibilidad con los proyectos implementados.

### 5.1 Estándares para el manejo de datos e información

Un estándar establece un sistema común de terminología y de definiciones para documentar datos. Idealmente las estructuras y definiciones de metadatos deben tener su referencia en un estándar. Hay muchos y variados estándares de metadatos disponibles. La razón de que existan tantos estándares es que los metadatos se emplean para diversas cosas.

¿Para qué estándares?

Los estándares permiten la localización rápida de cierto elemento. Si se utiliza un estándar, encontrar la información específica en un catálogo de metadatos será mucho más fácil que si no se utiliza ningún estándar.

- Los estándares permiten búsquedas automatizadas. Cuando se utilizan los estándares, las computadoras se pueden programar permitiendo buscar y encontrar conjuntos de datos útiles.

- Un beneficio de los estándares es que se han generado a través de un proceso de consulta (con otros "expertos") y ofrecen una base a partir de la cual pueden desarrollarse perfiles nacionales u orientados de acuerdo con materias.

- Ayudan a minimizar la duplicación de esfuerzos en la elaboración, recolección, procesamiento o distribución de la información.

La División de Seguridad de EMC, presentó los resultados de una encuesta realizada a más de 200 profesionales de TI Colombianos, en cuanto al uso de los estándares mundiales de TI, como parte los programas de seguridad de la información y cumplimiento de normas de su organización.

La encuesta titulada “Cumplimiento de TI Simplificado” fue realizada por RSA en Septiembre de 2008 en la conferencia Cisco Networkers en Cartagena, y en ésta se demostró que las organizaciones colombianas poseen una gran comprensión sobre cómo facilitar el cumplimiento de normas y regulaciones, apoyándose en la implementación de iniciativas basadas en estándares y/o mejores practicas como ISO 27002 e ITIL.

La encuesta incluyó resultados obtenidos de instituciones financieras reguladas por la Superintendencia Financiera de Colombia, quien ha emitido normas mínimas obligatorias de calidad y seguridad para manejo de la información confidencial de clientes.

Requisitos de calidad y seguridad de información como estos, surgen constantemente y los negocios de todo el mundo se esfuerzan por establecer programas proactivos para la seguridad y el cumplimiento de normas.

ISO 27002 es un estándar de la industria que se estableció para brindar lineamientos para iniciar, implementar, mantener y mejorar los sistemas de administración de seguridad y los procesos dentro de una organización.

ITIL es un conjunto de conceptos y políticas que organiza el enfoque para administrar la tecnología de la información y adopta los códigos de prácticas de ISO, para administración de la seguridad de la información.

La investigación demuestra que las organizaciones que comprenden los puntos en común entre ISO 27002 y los requisitos específicos de cada país, como el emitido por la Superintendencia Financiera de Colombia, están mejor posicionadas para garantizar que sus soluciones tecnológicas puedan ser reutilizadas, lo que permite mayor eficacia, uniformidad y disminución de costos.

Una metodología basada en estándares puede satisfacer el cumplimiento de los requisitos u otras regulaciones y también centralizar múltiples iniciativas de TI. El resultado: los negocios se benefician por medio de la disminución de controles redundantes y el aprovechamiento de las inversiones en tecnología.

“En la actualidad, los negocios se enfrentan con el complejo desafío de demostrar y mantener el cumplimiento de múltiples regulaciones”, comentó Jorge Cortés, Gerente de Ventas de RSA en Colombia. “La encuesta revela que las organizaciones colombianas están usando un enfoque sofisticado para resolver estos problemas, mediante la implementación de un solo estándar estratégico, basado en las mejores prácticas mundiales. Este enfoque eliminará muchos ciclos repetitivos por los cambios y el desarrollo constantemente de requisitos legales y regulatorios”.

De los principales beneficios obtenidos al aprovechar los estándares mundiales, los encuestados afirmaron que el seguimiento de las normas ISO mejorará significativamente la seguridad de su organización (23%) y simplificará y optimizará el cumplimiento de normas (21%).

Las ventajas de un enfoque integral, basado en estándares para la seguridad de TI, es que excede el cumplimiento de cualquier regulación establecida y contribuye con la seguridad integral y la eficacia operacional. La adopción de un estándar mundial también puede ayudar a la organización a adaptar la seguridad de la información a la toma de decisiones estratégicas y a las políticas de administración de riesgos de manera más específica.

### 5.2 Estándares de análisis, diseño e implementación de sistemas

El valor creciente de la información y de los sistemas de tecnologías de la información que la soportan, su omnipresencia y su carácter de instrumento esencial para el desarrollo económico y social de nuestra sociedad, las dependencias que se dan, y los riesgos generados, conducen todos ellos a la necesidad de adoptar políticas, procedimientos, prácticas y medidas organizativas y técnicas capaces de proteger la información y de gestionar la seguridad de los sistemas respondiendo a las amenazas existentes; capaces de garantizar dimensiones esenciales de la seguridad como la confidencialidad, la integridad, la disponibilidad y la autenticidad; de satisfacer la confianza depositada en los productos y sistemas, en la información necesaria para la toma de decisiones y en las posibles expectativas en cuanto a oportunidades de innovación y adaptación; así como de satisfacer los posibles requisitos legales, sean éstos de carácter horizontal o sectorial.

La dependencia de los sistemas de información preocupa cada vez más a la sociedad ya que genera riesgos debidos a la propia complejidad de los sistemas, a posibles accidentes, errores o ataques, a la constante evolución en un entorno cambiante, o a un posible uso irresponsable de los mismos. La materialización de estos riesgos puede afectar a la propia continuidad de los servicios (internos y externos), a la protección de la información en general y, en particular, de los datos de carácter personal, así como a la propia validez y eficacia de los actos que se apoyan en transacciones electrónicas, por ejemplo de administración o comercio electrónico.

Los diversos actores afectados, particulares, administraciones públicas y empresas, reclaman seguridad y, en definitiva, confianza en el uso de los sistemas de tecnologías de la información.

Los pasos a dar para garantizar la seguridad de los sistemas de tecnologías de la información se orientan a la implantación de una gestión continua de la seguridad, a la adopción de controles y salvaguardas organizativas y técnicas que garanticen aspectos tales como la continuidad de su funcionamiento, la protección de la información, la validez de las transacciones electrónicas, la conformidad con el marco normativo y contractual correspondiente, con condiciones tecnológicas (estándares) determinadas, el aseguramiento en cuanto a un uso adecuado y optimizado de los recursos, y, en general, la satisfacción de aquellos requisitos que contribuyen al logro de los objetivos de la organización.

Se pone de manifiesto, también, la necesidad o, en su caso, obligación de demostrar en la propia organización y ante terceros que se realiza una gestión competente, efectiva y continua de la seguridad en el marco de los riesgos detectados y de que se han adoptado aquellas medidas adecuadas y proporcionadas a los riesgos a los que está expuesta la organización.

Todo lo anterior demanda la existencia de un conjunto articulado, sistemático, estructurado, coherente y lo más completo posible de normas que sirvan de vocabulario y lenguaje común, de unificación de criterios, de modelo, especificación y guía para su uso repetido que permitan satisfacer las necesidades y expectativas de la sociedad en materia de construcción, mantenimiento y mejora de la seguridad de la información y de los sistemas que la soportan, aportando a la vez racionalización, disminución de costes, mejoras en competitividad y calidad e incluso nuevas oportunidades.

En los últimos seis años, se ha producido un incremento de la atención a la seguridad de los sistemas de información, atención a la que no han sido ajenos los Organismos de normalización que están ampliado notablemente sus catálogos de normas disponibles en esta materia. Así, se viene desarrollando una colección significativa de normas en el campo de la seguridad de las tecnologías de la información, que refleja también la evolución de la normalización en general, en la medida en que, junto con el enfoque tradicional de desarrollo de normas centradas en aspectos de la tecnología, se viene produciendo el desarrollo de normas relacionadas con prácticas de gestión, servicios y gestión de riesgos.

Este incremento de la atención a la seguridad de la información y de las tecnologías asociadas, correlativo con el desarrollo de la sociedad de la información en general, y de la administración electrónica en particular, viene teniendo reflejo también en actuaciones de la OCDE y la Unión Europea.

Así, el documento Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información: hacia una cultura de Seguridad señala que los Gobiernos deberían desarrollar políticas que recojan las buenas prácticas en la gestión de la seguridad y en la evaluación de riesgos.

A este respecto, indica que pueden usarse normas de gestión de la seguridad de la información reconocidos internacionalmente, tales como las normas ISO y normas específicas de la industria, para establecer sistemas de gestión de la seguridad eficaces.

En la Unión Europea, la Comunicación de la Comisión de las Comunidades Europeas sobre Seguridad de las redes y de la información: Propuesta para un enfoque político europeo (COM(2001) 298 final), propone una serie de medidas y acciones.

En particular, se refiere a cuestiones tales como las siguientes:

- Los estados miembros deberán fomentar el uso de mejores prácticas basadas en medidas existentes como ISO/IEC 17799.

- Se invita a las organizaciones de normalización europeas a que aceleren sus trabajos sobre interoperabilidad, para el apoyo a la normalización y certificación orientadas al mercado.

- Se invita a los estados miembros a que fomenten el uso de procedimientos de certificación y de acreditación de normas europeas e internacionales generalmente aceptadas que favorezcan el reconocimiento mutuo de certificados.

- Las administraciones públicas no deben tan solo prever requisitos de seguridad para la tecnología de los sistemas de información y comunicación, sino también desarrollar una cultura de seguridad en el seno de la organización. Ello se puede conseguir a través del establecimiento de "políticas de seguridad de la organización" hechas a medida para la institución de que se trate.

- Los estados miembros deberían incorporar soluciones eficaces e interoperables en materia de seguridad de la información como requisito básico para sus actividades en el campo de la administración y contratación pública electrónicas.

La administración, en sus proyectos de seguridad, tiene presente la normalización en seguridad de las tecnologías de la información, y expresa, además, su interés en el avance y madurez de las normas.

Esta normalización se aplica, por ejemplo, en proyectos relativos al establecimiento de políticas de seguridad, a la realización de planes directores de seguridad, y a la implantación de sistemas de gestión de seguridad de la información, entre otros.

Además, en el ámbito de la Administración General del Estado las normas se vienen teniendo presentes en instrumentos tales como los siguientes:

- Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades (Criterios SNC), en los que se exponen entre otras cuestiones, las pautas para la seguridad y normalización en lo servicios electrónicos prestados por los órganos y entidades del ámbito de la Administración General del Estado.

En los Criterios SNC se recogen normas tales como:

- UNE ISO/IEC 17799:2002, “Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información”.
- ISO/IEC 13335:2004, “Information technology - Security techniques - Management of information and communications technology security”.
- ISO/IEC 15408:1999, “Information technology - Security techniques - Evaluation criteria for IT security”.

- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT v2).

  En MAGERIT v2 se han tenido en cuenta normas tales como:

- ISO/IEC 17799:2005, “Information technology – Security techniques – Code of practice for information security management”.
- UNE ISO/IEC 17799:2002 – “Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información”.
- ISO/IEC Guide 73:2002, “Risk management – Vocabulary – Guidelines for use in Standards”.
- ISO/IEC TR 15443:2005, “Information technology -- Security techniques -- A framework for IT security assurance”.

- Herramienta PILAR, que soporta la realización del análisis y gestión de riesgos siguiendo la metodología MAGERIT v2.

Se tienen presentes las mismas normas que para MAGERIT v2.

- Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.
- ISO/IEC 15408, “Evaluation criteria for IT security”.
- ISO/IEC 18045:2005, “Methodology for IT security evaluation”.

### 5.3 Estándares de operación de sistemas

La naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditorías, requieren el desarrollo y la promulgación de Normas Generales para la Auditoría de los Sistemas de Información.

La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

A continuación, la descripción de los dos principales objetivos de una auditoría de sistemas, que son, las evaluaciones de los procesos de datos y de los equipos de cómputo, con controles, tipos y seguridad.

En el caso de la auditoría en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos:

- ✓ Evaluación de los sistemas y procedimientos.
- ✓ Evaluación de los equipos de cómputo.

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

Consta de:

- ➢ Evaluación de los sistemas y procedimientos
  - o Evaluación de los diferentes sistemas en operación (flujo de información, procedimientos, documentación, redundancia, organización de archivos, estándares de programación, controles, utilización de los sistemas).
  - o Evaluación del avance de los sistemas en desarrollo y congruencia con el diseño general.
  - o Evaluación de prioridades y recursos asignados (humanos y equipos de cómputo).
  - o Seguridad física y lógica de los sistemas, su confidencialidad y respaldos.

- Evaluación de los equipos de cómputo
  - Capacidades.
  - Utilización.
  - Nuevos proyectos.
  - Seguridad física y lógica.
  - Evaluación física y lógica.

- Controles administrativos en un ambiente de procesamiento de datos

La máxima autoridad del Área de Informática de una empresa o institución debe implantar los siguientes controles que se agruparan de la siguiente forma:

- Controles de preinstalación

Hacen referencia a procesos y actividades previas a la adquisición e instalación de un equipo de computación y obviamente a la automatización de los sistemas existentes.

Objetivos:

- ✓ Garantizar que el hardware y el software se adquieran siempre y cuando tengan la seguridad de que los sistemas computarizados proporcionaran mayores beneficios que cualquier otra alternativa.
- ✓ Garantizar la selección adecuada de equipos y sistemas de computación.
- ✓ Asegurar la elaboración de un plan de actividades previo a la instalación.

Acciones a seguir:

- ✓ Elaboración de un informe técnico en el que se justifique la adquisición del equipo, software y servicios de computación, incluyendo un estudio costo – beneficio.
- ✓ Formación de un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación.
- ✓ Elaborar un plan de instalación de equipo y software (fechas, actividades, responsables) el mismo que debe contar con la aprobación de los proveedores del equipo.
- ✓ Elaborar un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios computacionales. Este proceso debe enmarcarse en normas y disposiciones legales.
- ✓ Efectuar las acciones necesarias para una mayor participación de proveedores.
- ✓ Asegurar respaldo de mantenimiento y asistencia técnica.

- Controles de organización y planificación

Se refiere a la definición clara de funciones, línea de autoridad y responsabilidad de las diferentes unidades del área PAD, en labores tales como:

- ✓ Diseñar un sistema.
- ✓ Elaborar los programas.
- ✓ Operar el sistema.
- ✓ Control de calidad.
- ✓ Se debe evitar que una misma persona tenga el control de toda una operación.

Acciones a seguir:

- ✓ La unidad informática debe estar al más alto nivel de la pirámide administrativa de manera que cumpla con sus objetivos, cuente con el apoyo necesario y la dirección efectiva.
- ✓ Las funciones de operación, programación y diseño de sistemas deben estar claramente delimitadas.
- ✓ Deben existir mecanismos necesarios a fin de asegurar que los programadores y analistas no tengan acceso a la operación del computador y los operadores a su vez, no conozcan la documentación de programas y sistemas.
- ✓ Debe existir una unidad de control de calidad, tanto de datos de entrada como de los resultados del procesamiento.
- ✓ El manejo y custodia de dispositivos y archivos magnéticos deben estar expresamente definidos por escrito.
- ✓ Las actividades del PAD deben obedecer a planificaciones a corto, mediano y largo plazo sujetos a evaluación y ajustes periódicos "Plan Maestro de Informática".
- ✓ Debe existir una participación efectiva de directivos, usuarios y personal del PAD en la planificación y evaluación del cumplimiento del plan.
- ✓ Las instrucciones deben impartirse por escrito.

- Controles de sistemas en desarrollo y producción

Se debe justificar que los sistemas han sido la mejor opción para la empresa, bajo una relación costo – beneficio que proporcionen oportuna y efectiva información, que los sistemas se han desarrollado bajo un proceso planificado y se encuentren debidamente documentados.

Acciones a seguir:

- ✓ Los usuarios deben participar en el diseño e implantación de los sistemas pues aportan conocimiento y experiencia de su área y esta actividad facilita el proceso de cambio.
- ✓ El personal de auditoría interna / control debe formar parte del grupo de diseño para sugerir y solicitar la implantación de rutinas de control.

- ✓ El desarrollo, diseño y mantenimiento de sistemas obedece a planes específicos, metodologías, estándares, procedimientos y en general a normatividad escrita y aprobada.
- ✓ Cada fase concluida debe ser aprobada documentadamente por los usuarios mediante actas u otros mecanismos a fin de evitar reclamos posteriores.
- ✓ Los programas antes de pasar a producción deben ser probados con datos que agoten todas las excepciones posibles.
- ✓ Todos los sistemas deben estar debidamente documentados y actualizados. La documentación deberá contener:

- Informe de factibilidad.
- Diagrama de bloque.
- Diagrama de lógica del programa.
- Objetivos del programa.
- Listado original del programa y versiones que incluyan los cambios efectuados con antecedentes de pedido y aprobación de modificaciones.
- Formatos de salida.
- Resultados de pruebas realizadas.

- ✓ Implantar procedimientos de solicitud, aprobación y ejecución de cambios a programas, formatos de los sistemas en desarrollo.
- ✓ El sistema concluido será entregado al usuario previo entrenamiento y elaboración de los manuales de operación respectivos.

- o Controles de procesamiento

Los controles de procesamiento se refieren al ciclo que sigue la información desde la entrada hasta la salida de la información, lo que conlleva al establecimiento de una serie de seguridades para:

- ✓ Asegurar que todos los datos sean procesados.
- ✓ Garantizar la exactitud de los datos procesados.
- ✓ Garantizar que se grabe un archivo para uso de la gerencia y con fines de auditoría.
- ✓ Asegurar que los resultados sean entregados a los usuarios en forma oportuna y en las mejores condiciones.

Acciones a seguir:

- ✓ Validación de datos de entrada previo procesamiento debe ser realizada en forma automática: clave, dígito auto verificador, totales de lotes.
- ✓ Preparación de datos de entrada debe ser responsabilidad de usuarios y consecuentemente su corrección.

- ✓ Recepción de datos de entrada y distribución de información de salida debe obedecer a un horario elaborado en coordinación con el usuario, realizando un debido control de calidad.

- ✓ Adoptar acciones necesarias para correcciones de errores.

- ✓ Analizar conveniencia costo – beneficio de estandarización de formularios, fuente para agilizar la captura de datos y minimizar errores.

- ✓ Los procesos interactivos deben garantizar una adecuada interrelación entre usuario y sistema.

- ✓ Planificar el mantenimiento del hardware y software, tomando todas las seguridades para garantizar la integridad de la información y el buen servicio a usuarios.

- o Controles de operación

Abarcan todo el ambiente de la operación del equipo central de computación y dispositivos de almacenamiento, la administración de la Cintoteca y la operación de terminales y equipos de comunicación por parte de los usuarios de sistemas on line.

Los controles tienen como fin:

- ✓ Prevenir o detectar errores accidentales que puedan ocurrir en el centro de cómputo durante un proceso.

- ✓ Evitar o detectar el manejo de datos con fines fraudulentos por parte de funcionarios del PAD.

- ✓ Garantizar la integridad de los recursos informáticos.

- ✓ Asegurar la utilización adecuada de equipos acorde a planes y objetivos.

Acciones a seguir:

- ✓ El acceso al centro de cómputo debe contar con las seguridades necesarias para reservar el ingreso al personal autorizado.

- ✓ Implantar claves o passwords para garantizar operación de consola y equipo central (mainframe), a personal autorizado.

- ✓ Formular políticas respecto a seguridad, privacidad y protección de las facilidades de procesamiento ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación y como responder ante esos eventos.

- ✓ Mantener un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos.

- ✓ Los operadores del equipo central deben estar entrenados para recuperar o restaurar información en caso de destrucción de archivos.

- ✓ Los backups no deben ser menores de dos (padres e hijos) y deben guardarse en lugares seguros y adecuados, preferentemente en bóvedas de bancos.

- ✓ Se deben implantar calendarios de operación a fin de establecer prioridades de proceso.

- ✓ Todas las actividades del centro de cómputo deben normarse mediante manuales, instructivos, normas y reglamentos.
- ✓ Las instalaciones deben contar con sistema de alarma por presencia de fuego, humo, así como extintores de incendio, conexiones eléctricas seguras, entre otras.
- ✓ Instalar equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores pico, UPS, generadores de energía.
- ✓ Contratar pólizas de seguros para proteger la información, equipos, personal y todo riesgo que se produzca por casos fortuitos o mala operación.

### 5.4 Estándares sobre los procedimientos de entrada de datos, procesamiento de información y emisión de resultados

De una forma panorámica los principales ámbitos de normalización son los relativos al sistema de gestión de seguridad de la información, a las técnicas y mecanismos, sean o no criptográficos, y a la evaluación de la seguridad de las tecnologías de la información y aspectos asociados, según se refleja en el gráfico siguiente (figura 1), que también recoge la presencia de ámbitos que, de forma creciente, demandan una atención especializada, como la gestión de identidad y privacidad y los servicios y controles de seguridad, aunque se apoyen, así mismo, en los tres ámbitos principales citados.

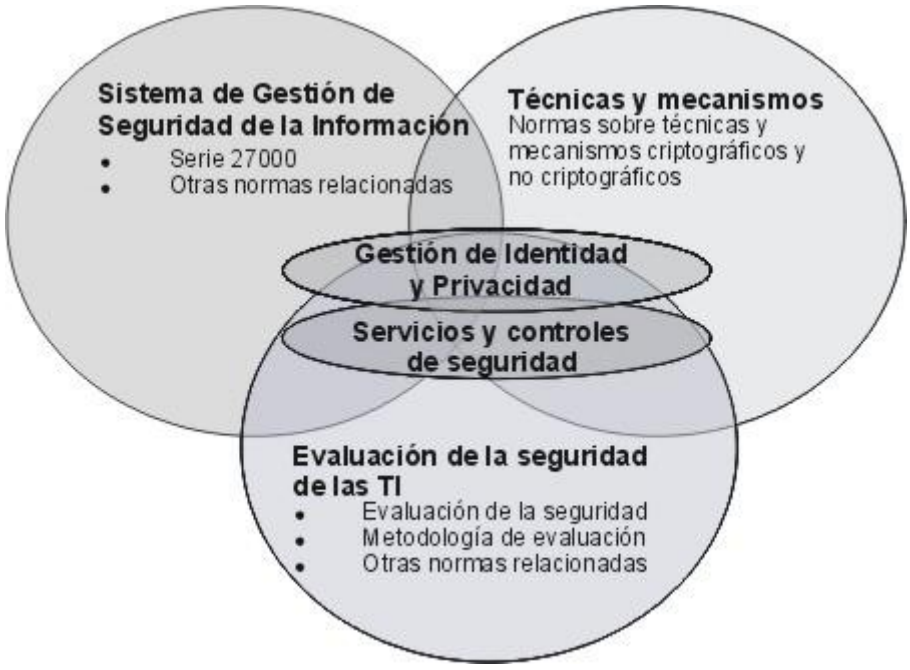


Figura 1: Panorámica general de ámbitos de normalización en ISO/IEC SC27

Normas de gestión de seguridad de la información

Perspectiva general:

En 2004 se crea la serie 27000, con el objetivo de contribuir a la mejor identificación y ordenación de las normas de gestión de seguridad de la información, y satisfacer cuestiones tales como las siguientes:

- Proporcionar un marco homogéneo de normas y directrices.
- Proporcionar requisitos, metodologías y técnicas de valoración.
- Evitar el solapamiento de las normas y favorecer la armonización.
- Alinearse con los principios generalmente aceptados relativos al gobierno de las organizaciones.
- Ser consistente con las Directrices de Seguridad y de Privacidad de la OCDE.
- Usar lenguaje y métodos comunes.
- Facilitar la flexibilidad en la selección e implantación de controles.
- Ser consistente con otras normas y directivas de ISO.

El estado de situación de la serie 27000 es el siguiente:

| Numeración | Estado de situación |
|---|---|
| 27000 | En proyecto: Information security management fundamentals and vocabulary. |
| 27001 | ISO/IEC IS 27001:2005 Information technology Security techniques - Information security management systems. Norma disponible desde el 14 de octubre de 2005. |
| 27002 | ISO/IEC IS 17799:2005Information technology – Security techniques – Code of practice for information security management.<br>Norma disponible desde el 10 de junio de 2005. Está previsto que la numeración '27002' entre en vigor en 2007. |
| 27003 | En proyecto: Information security management system implementation guidance. |
| 27004 | En proyecto: Information technology Security techniques - Information security management measurements. |
| 27005 | En proyecto: Information Security Risk Management. |
| 27006 | ISO/IEC IS 27006:2007Requirements for the accreditation of bodies providing certification of information security management systems.<br>Norma disponible desde el 13 de febrero de 2007. |
| 27007 | En proyecto: Auditing Information Security Management Systems against ISO 27001 |
| 27008 | En reserva. |
| 27009 | En reserva. |
| 27011 | En proyecto. Information security management guidelines for telecommunications |

Informes y normas UNE

En el ámbito de la normalización nacional, la creación de un cuerpo de normas e informes UNE viene tratando principalmente, hasta la fecha, la gestión de la seguridad de la información:

| Informes y normas UNE | |
|---|---|
| Informe UNE 71501-1:2001 | Guía para la gestión de la seguridad de la tecnología de la información. Conceptos y modelos para la seguridad de la tecnología de la información. |
| Informe UNE 71501-2:2001 | Guía para la gestión de la seguridad de la tecnología de la información. Gestión y planificación de la seguridad de la tecnología de la información. |
| Informe UNE 71501-3:2001 | Guía para la gestión de la seguridad de la tecnología de la información. Técnicas para la gestión de la seguridad de la tecnología de la información. |
| UNE 71502:2004 | Especificaciones de un sistema de gestión de la seguridad de la información. |
| UNE ISO/IEC 17799:2002 | Código de buenas prácticas para la gestión de la seguridad de la información. |

Sistema de gestión de seguridad de la información

Diversas normas promueven la aplicación de un sistema de procesos encaminado a gestionar la seguridad. Tal enfoque enfatiza la importancia de aspectos tales como los siguientes:

- La comprensión de los requisitos de seguridad de la información y la necesidad de establecer objetivos y una política para la seguridad de la información.
- La implantación y explotación de controles para gestionar los riesgos relativos a la seguridad de la información en el contexto general de los riesgos globales de la organización.
- El seguimiento del rendimiento del sistema.
- La mejora continua basada en la medida de los objetivos.

Tales normas adoptan el ciclo conocido como “Plan-Do-Check-Act” para especificar los requisitos del denominado Sistema de Gestión de Seguridad de la Información. A la fecha se dispone de las siguientes normas:

- UNE 71502:2004 Especificaciones para los sistemas de gestión de la seguridad de la información.
- ISO/IEC 27001:2005 Information Technology – Security techniques – Information security management systems – Requirements.

Se encuentra en elaboración la norma UNE equivalente a ISO/IEC 27001:2005 con vistas a retirar a corto plazo la norma UNE 71502:2004.

La norma UNE 71502:2004 define un Sistema de Gestión de la Seguridad de la Información (SGSI) como aquel “sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. El sistema es la herramienta de que dispone la dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad (integridad, confidencialidad y disponibilidad, asignación de responsabilidad, autenticación). Proporciona mecanismos para la salvaguarda de los activos de información y de los sistemas que los procesan, en concordancia con las políticas de seguridad y planes estratégicos de la organización.”

Mientras que la norma ISO/IEC 27001:2005 lo define como:

“Parte del sistema global de gestión, que sobre la base de un enfoque basado en los riesgos, se ocupa de establecer, implantar, operar, seguir, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye estructuras organizativas, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.”

La implantación de un SGSI permite a una organización lo siguiente:

- ✓ Conocer los riesgos.
- ✓ Prevenir, reducir, eliminar o controlar los riesgos mediante la adopción de los controles adecuados.
- ✓ Asegurar el cumplimiento de la legislación en materias tales como la protección de los datos de carácter personal, los servicios de la sociedad de la información o la propiedad intelectual, entre otras.

## 5.5 Estándares en el sistema de teleinformática

Introducción

Entendemos como teleinformática como el conjunto de elementos y técnicas que permiten la transmisión automática de datos.

El inconveniente principal de las redes de computadoras propietarias consiste en su dependencia de la tecnología. Así, cada fabricante recurre a unas soluciones hardware distinto a la hora de implementar su red, haciendo casi imposible la conexión a la red de computadoras de otros fabricantes. Es por ello que, tras varios años de lucha entre fabricantes, se llegue a la conclusión de que el problema debe solucionarse a más alto nivel. En ese momento surge la problemática de la interconexión de redes.

Este modelo de funcionamiento consiste en que redes diferentes utilicen a alto nivel protocolos comunes, que permitan ignorar en el ámbito de usuario las diferentes implementaciones a bajo nivel.

Para ello resulta imprescindible establecer de forma estándar los protocolos de comunicaciones utilizados para la interconexión de redes. Gracias a ellos se da el siguiente paso, llegando a la interconexión de redes, o Internet.

Nomenclaturas

La teleinformática no se ha desarrollado como una disciplina teórica, sino que ha ido evolucionando gracias, en gran medida, a implementaciones realizadas por laboratorios de investigación, universidades

y la empresa privada. Además, la aproximación al problema ha sido enfocada de forma distinta por diferentes organismos, por lo que los conceptos utilizados son distintos.
Por todo ello, no existe una terminología única que permita denominar de forma inequívoca a los componentes de estos sistemas.

En el campo de las nomenclaturas, hay dos de las más empleadas:

- Nomenclatura ARPA

A comienzos de los 60's en Estados Unidos se puso en marcha el proyecto ARPANET, patrocinado por ARPA (Advanced Research Proyect Agency), dependiente del Departamento de Defensa. Este proyecto militar perseguía la creación de una red de interconexión entre centros militares y universidades. Con el tiempo, esta red se convirtió en Internet.

El modelo ARPA especifica la existencia de computadoras terminales (Hosts) dispuestos para ejecutar tareas de usuario, y que son los usuarios de la comunicación. Para interconectar estas computadoras se utiliza una sub-red de comunicaciones, que une a los Hosts entre sí. Esta sub-red se encuentra formada por dos tipos de elementos: Las líneas y los procesadores de comunicaciones.

Es necesario destacar que para ARPA son igualmente partes del Host los posibles elementos de comunicaciones integrados en el sistema, como pueden ser tarjetas de red o dispositivos MÓDEM, e incluso los denominados procesadores frontales de comunicaciones ( front-end processors) cuya única misión consiste en descargar de las tareas de comunicaciones al resto del sistema.

Los procesadores de comunicaciones, también conocidos como nodos, computadoras de comunicaciones e I.M.P's ( Interface Message Processors), son los encargados de que la información transmitida por los Host llegue a su destino. Para ello realizan tareas de encaminamiento de la información a través de la sub-red. Cada IMP se encuentra permanentemente preparado para la recepción por cualquiera de sus líneas. Cuando llega una unidad de información por alguna de sus entradas, evalúa en función de la dirección destino de la misma y el conocimiento del IMP sobre la red cuál debe ser la línea de salida. A cada uno de estos procesos de recepción, evaluación y transmisión se le denomina salto ó hop. Eventualmente, y tras un número finito de hops, la información será entregada por el IMP correspondiente al host destino.

Las líneas de comunicaciones interconectan entre sí a los procesadores de comunicaciones y a éstos con los Hosts. Pueden ser de dos tipos: líneas punto a punto o multipunto.

Las líneas punto a punto unen entre sí dos extremos fijos. Habitualmente existirá un emisor y un receptor. Son, por tanto, eminentemente unidireccionales, aunque con una gestión adecuada es posible utilizarlas en ambos sentidos no simultáneamente.

Cuando en una línea de comunicaciones existe un emisor y un receptor fijos, es decir, la información viaja en un sólo sentido, se dice que la línea es simple (simplex). Por el contrario, cuando el papel de emisor puede ser adoptado por ambos equipos, pero no simultáneamente se dice que la línea es semiduplex (half-duplex).

Para permitir la comunicación bidireccional simultánea entre dos equipos serían necesarias dos comunicaciones simples. Este tipo de líneas se denomina duplex (full-duplex).

Uno de los aspectos más importantes de las redes con líneas punto a punto es la topología, es decir, cómo se interconectan entre sí todos los nodos. De la topología dependerán en gran medida las prestaciones de la red, su coste, su facilidad de ampliación, sus posibilidades de congestión.

Las líneas multipunto comunican varios nodos, siendo posible que cualquiera de ellos utilice la línea tanto como emisor como receptor. Esto permite reducir el número de líneas de comunicaciones, y

permitir que todos los nodos se encuentren a una distancia de un único hop. Sin embargo, resulta imposible que una única línea sea utilizada simultáneamente por más de un nodo, por lo que es necesario establecer algunas reglas. El mecanismo de acceso al medio, es decir, qué acciones debe seguir un nodo para utilizar una línea multipunto, será el factor determinante de la velocidad de la red. La fiabilidad del sistema, por el contrario, será muy elevada con respecto a fallos en los nodos pero nula en cuanto a fallos en la línea común.

- Nomenclatura ITU

ITU (International Telecommunications Union) es un organismo internacional que agrupa a las compañías de telecomunicaciones, tales como Telefónica, British Telecomm, ATT.

Esta organización procede de la antigua CCITT (Comité Consultivo Internacional de Teléfonos y Telégrafos), con las mismas funciones y múltiples estándares. Sus trabajos, respaldados por la ONU, establecieron una nomenclatura según la cual se distinguen los siguientes elementos:

- Sub-red: Se trata de un elemento gestionado por los denominados proveedores del servicio, es decir, las compañías telefónicas. Por ello, no se describen los elementos que forman parte de ella.

- Equipos terminales de Datos (ETD´s): Son los elementos que desean comunicarse, típicamente computadores que ejecutan procesos de usuario, aunque existen otras opciones (terminales tonitos, equipos de videotexto). También se denominan DTE ( Data Terminal Equipement) Equipos terminales del circuito de Datos ( ETCD) ó DCE (Data Circuit Terminal Equipement). Son los elementos que permiten la interconexión entre el DTE y la sub-red. Un ejemplo de esto son los MÓDEM telefónicos.

Estándares

En el mundo de la teleinformática resulta muy frecuente la interconexión de máquinas de distintos fabricantes. Para ello es necesario que todos los computadores involucrados en la comunicación sean capaces de transmitir e interpretar la información utilizando los mismos protocolos. Para conseguir esto aparecen los estándares de comunicaciones.

Podemos definir un estándar como una normativa comúnmente aceptada por fabricantes y usuarios. Así, podremos distinguir dos tipos de estándares:

- Estándares que han sido promovidos por algún organismo, tanto nacional como internacional.

- Estándares que proceden de fabricantes y que, sin ser obra de ningún organismo, se imponen por motivos técnicos o de marketing.

Los primeros son los conocidos como estándares de jure, mientras que los segundos son los estándares de facto.

Los organismos emisores de estándares de jure son los siguientes:

- ITU ( International Telecommunication Union): Es el organismo que agrupa a las compañías proveedoras de servicios telefónicos de multitud de países, entre ellas Telefónica. Procede del antiguo CCITT (Comité Consultivo Internacional de Teléfonos y Telégrafos). Sus normas son sobre todo relativas a DCE´s y su conexión con los DTE´s. Se denominan mediante una letra y un número. (p.e. X.25, X.500, V.22, V32).

- IEEE (Institute of Electrical and Electronics Engineers): A pesar de no ser un organismo internacional.

- ISO ( International Standards Organization): La organización internacional de estandarización agrupa a los organismos nacionales de casi todos los países, entre los que destacan ANSI (American National Standards Institute), DIN (Alemania), AFNOR (Francia) , BSI (Gran Bretaña).

- IAB (Internet Arquitecture Board): Este organismo supervisa las normas empleadas en Internet. Consta básicamente de dos organismos: IRTF (Internet Research Task Force) e IETF (Internet Engineering Task Force), encargadas respectivamente de la investigación y el desarrollo de estándares en Internet.

El mecanismo para la creación de las normas pasa por los RFC´s (Request For Comments), un documento público al cual todo usuario de Internet puede hacer críticas. Tras varias fases, este documento pasará al estado STD, siendo considerado desde entonces un estándar establecido.

Los estándares de facto suelen ser propuestas por un fabricante y adoptadas por otros para sus productos. Responden a la falta de normativa en bastantes de los aspectos de la informática en los primeros tiempos. Ejemplos de estándares de este tipo son el lenguaje de comandos Hayes o el interfaz Centronics para impresoras. Estos estándares suelen acabar convertidos en estándares de jure cuando algún organismo de los anteriormente citados los adopta.

### 5.6 Estándares de documentación

Open Document?

El Formato de Documento Abierto para Aplicaciones Ofimáticas de OASIS (en inglés, OASIS Open Document Format for Office Applications), también referido como Open Document u ODF, es un formato de fichero estándar para el almacenamiento de documentos ofimáticos tales como hojas de cálculo, memorandos, gráficas y presentaciones.

Su desarrollo ha sido encomendado a la organización OASIS (acrónimo de Organization for the Advancement of Structured Information Standards) y está basado en un esquema XML inicialmente creado por Open Office**?**.org.

Open Document fue aprobado como un estándar OASIS el 1 de mayo de 2005. Asimismo fue publicado el 30 de noviembre de 2006 como estándar ISO 26300, alcanzando la fase 60.60 del proceso de estandarización.

Por otra parte la versión 1.1 de la especificación fue aprobada el 25 de octubre de 2006 por el comité de estandarización de OASIS. El estándar fue desarrollado públicamente por un grupo de organizaciones, es de acceso libre, y puede ser implementado por cualquiera sin restricción. El formato Open Document pretende ofrecer una alternativa abierta a los formatos de documentos propiedad de Microsoft cuyos requisitos de licencia impiden su empleo a diversos competidores.

La motivación principal para usar formatos estándar reside en que las organizaciones e individuos que lo hacen evitan la dependencia de un único proveedor de software, permitiéndoles cambiar de entorno informático si su proveedor actual es expulsado del mercado o cambia su modelo de licencia en términos menos favorables para el cliente.

Open Document es el primer estándar para documentos ofimáticos implementado por distintos competidores, visado por organismos de estandarización independientes y susceptibles de ser implementado por cualquier proveedor.

Estandarización y licencia

La versión 1.0 de la especificación de Open Document fue aprobada como estándar OASIS en mayo de 2005 y está disponible para descarga y uso libres. La especificación se puede licenciar en términos recíprocos por cualquier parte siempre que no estén sometidos a cuotas. Los términos de la licencia son equivalentes a los promovidos por otras organizaciones de normalización, tales como el W3C, y pretenden evitar el conflicto entre las cuestiones relativas a la propiedad intelectual y la promoción de la innovación tecnológica.

El proceso de estandarización incluyó a desarrolladores de muchas aplicaciones de oficina o relacionadas con sistemas de documentación, incluyendo (en orden alfabético):

- Adobe (Framemaker, Distiller).
- Arbortext (Arbortext Enterprise Publishing System).
- Corel (Word Perfect) • IBM (Lotus 1–2−3, Workplace).
- KDE (K Office**?**).
- Speed Legal**?** (Smart Precedent**?** enterprise document assembly system); producto y compañía después cambiaron de nombre a Exari.
- Sun Microsystems / Open Office.org (Open Office**?**).

El proceso de la estandarización de Open Document también incluyó a muchos usuarios, especialmente algunos con necesidad de manejar documentos complejos, o de poder recuperarlos bastante tiempo después de haber sido creados.

Algunos usuarios implicados en el proceso de la estandarización fueron (alfabéticamente):

- Boeing (documentos grandes y complejos).
- Intel (documentos grandes y complejos; desarrollan textos de prueba).
- National Archive of Australia (acceso a documentos mucho tiempo después de su composición).
- New York State Office of the Attorney General (documentos grandes y complejos que requieren acceso mucho tiempo después de su composición).
- Society of Biblical Literature (grandes documentos políglotas, con capacidad de acceso después de largo tiempo).

Microsoft también impone condiciones adicionales de licencia para usuarios de su formato; muchos creen que estas condiciones adicionales inhiben la competencia, y forman parte del intento de Microsoft de proteger su virtual monopolio en aplicaciones para oficina; otros esperan que los hechos obligarán a Microsoft a desistir del intento de imponer su propio formato, del mismo modo que se vio obligado en la década de 1990 a abandonar sus estándares de Internet para adoptar estándares abiertos.

Finalmente, en mayo de 2008, Microsoft anunció que, en algún momento del primer semestre de 2009, lanzará el Service Pack 2 (SP2) para Microsoft Office 2007, el cual incluirá, entre otros cambios, compatibilidad directa, relativamente integrada y completa, con los estándares ODF y PDF, permitiendo

incluso configurar ODF como formato por defecto en las principales aplicaciones de su paquete ofimático.

Las iniciativas de estandarización no sólo aseguran un mercado limpio y competitivo, sino que aseguran la interoperabilidad de las soluciones, preservando la competencia y la innovación.

Las recomendaciones incluyen:

- Los actores de la industria no involucrados aún en el Open Document Format de OASIS deben considerar participar en el proceso de estandarización a fin de alentar un amplio consenso de la industria en torno al formato.

- Microsoft debe considerar la publicación de un compromiso en el sentido de publicar y facilitar un acceso no discriminatorio a las versiones futuras de su especificación XML para Word.

- Microsoft debe considerar la conveniencia de remitir los formatos XML a un organismo internacional de estandarización de su elección.

- Se recomienda al sector público a proporcionar su información a través de varios formatos. Cuando por circunstancias o por elección se proporcione sólo un formato editable, éste debería ser uno en torno al que exista un consenso en la industria, como se demuestra por la adopción del formato como estándar. (TAC, 25 de mayo de 2004).

Open Document es ya un estándar reconocido por un organismo independiente (OASIS), y ha sido remitido a la ISO, sin que exista evidencia de que los formatos XML de Microsoft, o los antiguos DOC/PPT/XLS vayan a sufrir un proceso análogo.

Tal y como muchos esperaban ISO ha aceptado y aprobado Open Document por el procedimiento rápido, y ahora sólo queda que la Unión Europea establezca este formato como estándar ofimático ya que ha sido ratificado dicho estándar por ISO.

En noviembre de 2007 Holanda estableció, por ley, una fecha límite para las administraciones públicas para la adopción de estándares abiertos. Massachusetts A principios de 2005, Eric Kriss, Secretario de Administraciones Públicas y Hacienda de Massachusetts, estableció como uno de los principios de su administración el compromiso de utilizar formatos abiertos en la siguiente declaración:

“Es absolutamente imperativo para el sistema democrático de los EEUU que perdamos la práctica de tener nuestros documentos públicos cautivos en un formato exclusivo, sea éste el que sea, arriesgándonos a que en el futuro el documento sea quizás ilegible o esté sujeto a un sistema de licencias exclusivo que restrinja su acceso.”

El 21 de septiembre de 2005, Massachusetts se convirtió en el primer estado norteamericano en aprobar formalmente los diferentes formatos Open Document para su uso en los registros públicos, a la vez que se rechazaba el formato basado en XML propuesto por Microsoft, su principal proveedor actual, por no ser considerado abierto. Si Microsoft decide no dar soporte a Open Document para 2007, fecha límite definida por el Estado, se descalificará de consideración futura por el Estado de Massachusetts.

El objetivo principal es que las aplicaciones basadas en software ofimático cumplan estas especificaciones (tanto si es software licenciado, como si es de fuente abierta, o libre) y que de este modo muchos desarrolladores puedan hacer aportaciones al mercado de las TIC educacionales.

## 5.7 Estándares de mantenimiento

De la definición de mantenimiento del estándar IEEE 1219 cabe distinguir tres causas fundamentales que desencadenan las actividades de mantenimiento.

Las causas u origen de las actividades de mantenimiento del software pertenecen a tres grupos principales:

- Eliminación de defectos del producto software.

Las causas por tanto son todas ellas resultado de tener que modificar el software para que cumpla con los requisitos del usuario ya establecidos.

- Adaptar el producto software a.

Para que siga cumpliéndolos cuando cambia su entorno.

- Incluir mejoras en el diseño.

Cuando se quiere mejorar la manera en que los cumple.

Por otro lado, la definición anterior implica que el mantenimiento debido a los defectos es a posteriori, es decir, se desencadena cuando el defecto tiene como resultado un fallo que se detecta.

En ocasiones, se realizan actividades de mantenimiento preventivo, que intentan detectar y corregir fallos latentes (que se supone pueden existir, aunque aún no se han “manifestado”).

Estas causas tienen su correlación directa con las denominadas “categorías de mantenimiento”, que en el estándar ISO/IEC 147641 incluye las siguientes categorías definidas por Lientz y Swanson 2(1978) que son:

- Mantenimiento correctivo: modificaciones reactivas a un producto software hechas después de la entrega para corregir defectos descubiertos.

- Mantenimiento adaptativo: modificación de un producto software realizada después de la entrega para permitir que un producto software siga pudiéndose utilizar en un entorno diferente.

- Mantenimiento perfectivo: modificación de un producto software después de la entrega para mejorar el rendimiento o la mantenibilidad.

Una consecuencia importante de las definiciones anteriores es que no se considera mantenimiento a los cambios introducidos para incluir nuevos requisitos funcionales. No obstante, no hay un consenso unánime en este sentido, y de hecho, el concepto de evolución del software amplía el espectro del mantenimiento a cambios en un sentido amplio. De hecho, hay autores que consideran que el mantenimiento perfectivo sí incluye cambios en la funcionalidad.

Las categorías adaptativa y perfectiva son ambas mejoras, en contraposición el mantenimiento correctivo.

Por último, un estándar de mantenimiento del IEEE (1998) define una categoría adicional, la de mantenimiento de emergencia, cuando los cambios se deben hacer sin planificación previa, para mantener un sistema en operación. Todas las anteriores definiciones son las que se encuentran

habitualmente en los libros. No obstante, la clasificación más exhaustiva se encuentra en el artículo de Chapin (2001).