INSTITUTO POLITECNICO NACIONAL

"Escuela Superior de Computo"

Administración de Centros de Cómputo

CALIDAD

CARACTERISTICAS DE LA CALIDAD SEGÚN ISO 9126

Antes de detallar los procesos de calidad, vamos a describir los componentes de una especificación de calidad de software según el modelo definido en la norma ISO 9126 y el modelo extendido ISO para la calidad del software.

Características

Según la citada norma ISO 9126, define las características de calidad como “Un conjunto de atributos del producto software a través de los cuales la calidad es descrita y evaluada” Las características de calidad del software pueden ser precisas a través de múltiples niveles de subcaracterísticas.

Dicha norma define 6 características

Funcionalidad: Conjunto de atributos que se refieren a la existencia de un conjunto de funciones y sus propiedades específicas. Las funciones son tales que cumplen unos requerimientos o satisfacen unas necesidades implícitas.

Fiabilidad: Conjunto de atributos que se refieren a la capacidad del software de mantener su nivel de rendimiento bajo unas condiciones especificas durante un periodo definido.

Usabilidad: Conjunto de atributos que se refieren al esfuerzo necesario para usarlo, y sobre la valoración individual de tal uso por un conjunto de usuarios, usuarios definidos o implícitos.

Eficiencia: Conjunto de atributos que se refieren a las relaciones entre el nivel de rendimiento del software y la cantidad de recursos usados mediante unas condiciones predefinidas.

Mantenibilidad: Conjunto de atributos que se refieren al esfuerzo necesario para hacer modificaciones específicas.

Portabilidad: Conjunto de atributos que se refieren a la habilidad del software para ser transmitido desde un entorno a otro.

La norma incluye un anexo en el que desglosa en un conjunto de sub-características cada una de las características anteriormente citadas. Sin embargo este anexo puede considerarse informativo y no como parte oficial del estándar ISO 9126

El prefijo Sub nos hace destacar una parte importante del modelo ISO 9126. La calidad es modelizada en forma jerárquica.

Modelo ISO Extendido

EL modelo ISO extendido incluye al modelo ISO 9126 adicionando dos características más.

La valoración de estas características es útil para que el usuario pueda definir los requerimientos del producto utilizando solamente las características que emplee en la práctica.

Para algunos tipos de productos, hay determinadas características que no son significativas y las restantes no garantizan que con ellas comprendan todos los requerimientos de los productos, por lo que en cada caso habrá que completarlas con otras definiciones mas especificas para esos productos o situaciones.

No obstante el modelo tiene el nivel de abstracción suficiente como para que sea adaptable a la mayoría de las situaciones, siendo, además independiente de la tecnología.

Las características no pueden ser cuantificadas como tales y para cuantificarlas en alguna forma usaremos los Indicadores.

Para usar los indicadores deberemos definir un protocolo, de forma que mediante dicho protocolo podamos establecer la medida de la característica repetible. Este protocolo describirá los pasos que hay que dar para conseguir esta medida de forma tal que en las mismas situaciones obtengamos idénticos resultados.

Los indicadores que se describen en el modelo ISO extendido, sirven como punto de partida, no queriendo decir que dicha lista sea completa. En ella se pretenden presentar ideas para poder definir las especificaciones de calidad, siendo muy importante seleccionar los indicadores que mejor se adapten a la situación del servicio.

El protocolo de medida tiene como objetivo el reproducir los resultados de las mediciones de los indicadores. Según se ha indicado anteriormente, al describir los requerimientos de calidad del software. Se corre el peligro de una interpretación subjetiva del significado de calidad. Es, por tanto, de gran importancia acordar de una forma clara como medir los indicadores de forma que esta medida sea reproducible con los mismos resultados.

Ejemplo

Si deseamos medir el atributo facilidad de aprendizaje, que podemos definir como el esfuerzo de los usuarios para aprender a manejar una aplicación.

Podríamos hacer una cuantificación fácil si pudiéramos medir de una forma objetiva el factor de facilidad de aprendizaje de 7 sobre 10, pero este no sería muy descriptivo ni útil.
Podríamos buscar algún indicador de este atributo que estuviera presente en el producto software. Este indicador debe estar acompañado del protocolo de medida que describa los pasos a dar para asegurar la repetitividad de la medida.

En este ejemplo hemos tomado como indicador el Tiempo Medio de Aprendizaje, siendo el tiempo promedio que el usuario final de un determinado grupo necesita para aprender a trabajar con el producto software, mas el tiempo necesario de tutelaje.

El protocolo sería.

- Selección de un grupo representativo de usuarios.
- Preparación de un curso para este grupo, diseñado para este producto software o dar a este grupo la oportunidad de auto – enseñanza del producto.
- Definición del tiempo del curso o de la auto enseñanza, mas el tiempo de tutelaje necesario para conseguir su manejo o pasar con éxito un test.
- Calculo del número medio de horas.

Los valores obtenidos de las características se pueden representar de distintas maneras puede ser con graficas de barras o de tipo radio

El valor de los indicadores depende del propósito de la especificación de la calidad, pudiendo definirse diferentes valores. Es aconsejable usar una plantilla con estos valores. A continuación se expone un pequeño ejemplo de este tipo de plantilla.

Peor El peor límite aceptable en la escala, tal como un fallo total del sistema
Planificado Valor esperado del indicador que se considera un éxito.
Récord Máximo valor teórico o práctico de un indicador, valor límite pero no un requerimiento esperado.
Actual. Valor actual en el que el sistema que se está considerando a efectos posibles de comparaciones.

FLUJO DE TRABAJO EN UN DEPARTAMENTO DE SISTEMAS

Desarrollar sistemas informáticos que apoyen las funciones académicas (principalmente) y administrativas de las diferentes áreas de la Facultad, teniendo en cuenta una revisión integral de los procesos involucrados en dichas áreas a fin de resolver necesidades actuales y futuras con propuestas acordes a la realidad.

- Realizar investigaciones tecnológicas cuyos resultados sean evaluados para su utilización en la realizacion de los sistemas.

- Involucrar y capacitar a los alumnos de la Licenciatura en Informática que realizan su servicio social en el Departamento en el proceso de desarrollo de sistemas.

- Llevar una adecuada administración de los proyectos que se realizan en el departamento.

- Asesorar en cuestión del área de sistemas y desarrollo de software a las diferentes área de la Facultad que lo requieran.

- Realizar una eficiente y adecuada ejecución de las etapas del ciclo de desarrollo de sistemas, a través de la utilización de metodologías, técnicas y herramientas, que permitan obtener un proyecto exitoso:

- Análsis.
- Diseño.
- Desarrollo.
- Pruebas.
- Implantación.
- Mantenimiento.

Gestión de la configuración
Gestión de fallos
Gestión del rendimiento
Gestión de la seguridad
Gestión de la contabilidad
Métodos conceptuales.
Métodos de especificación.
Métodos de implementación.
Procesos de atención al cliente.
Procesos de desarrollo y operación de servicios y productos: Procesos de gestión de la red y de los sistemas.

RELACIONES CONTEXTUALES DE LA GESTIÓN DE SERVICIO CON OTROS PROCESOS DE LA EMPRESA

Relaciones con los procesos de negocio
Relaciones con los procesos de gestión de infraestructuras
Relaciones con otros proveedores externos

TÉCNICAS DE FLUJO DE TRABAJO

Introducción a las técnicas de flujo de trabajo (workflow).
Modelo de referencia de flujo de trabajo.
Características de los sistemas de información basados en flujos de trabajo (workflow).
Estándares de flujo de trabajo
Casos de estudio.

LA INTEGRACIÓN DE LA GESTIÓN DE SERVICIO

Necesidad de la integración de los servicios.
Principios generales de arquitectura para la integración de servicios.
Tecnologías disponibles para la integración de servicios.

ARQUITECTURAS DE INTERFAZ CON CLIENTES

Call centers
Help desk
Bases de datos de clientes
Sistemas IVR
Portales

PLATAFORMAS DE COMPUTACIÓN PARA LA GESTIÓN DE SERVICIOS.

Gestores de provisión de servicios
Gestores de problemas (Trouble Ticket Systems).
Gestores de órdenes de trabajo (Work Order Systems).
Gestores de calidad en los servicios (QoS) y de acuerdos de nivel de servicio (SLA).

Concepto de seguridad total.

Exigencias para incrementar la seguridad en computación.

Las empresas especializadas en servicios de asesoría para la seguridad en computación han proliferado, en mas de un caso son dirigidas por individuos que poseen antecedentes delictivos y han cometido robo o fraude en grandes instalaciones de computación, por lo tanto resulta claro que se ha desarrollado un área nueva de preocupación gerencial.

En algunas empresas y libros se define a la seguridad en computación a métodos tradicionales en las que abarcan a la seguridad física y contra incendios, por lo tanto muchas instituciones que han cubierto estas áreas viven una situación ficticia de seguridad, mientras que en realidad el nivel de seguridad se encuentra por debajo del aceptable.

En contraste con los antecedentes sobre la seguridad en computación, que generalmente es superficial, existen ciertos factores que han aumentado el nivel de seguridad que se requiere, los cuales se describen a continuación.

- **Concentración del procesamiento de aplicaciones mas grandes y de mayor complejidad**

La principal causa del incremento en los riesgos de computación probablemente sea el aumento en la cantidad de aplicaciones que se da a las computadoras y la consecuente concentración de información y procesamiento. La tendencia creciente hacia la incorporación de sistemas mayores y mas complejos que incluyen procesamiento en línea así como el uso de DB constituye un problema adicional.

La institución computarizada corre el riesgo de sufrir amnesia corporativa, debido a algún desastre en las computadoras y de que sobrevenga una suspensión prolongada del procesamiento.

- **Dependencia en el personal clave**

Esta situación existe en todas las funciones de la institución, la dependencia de individuos clave, algunos de los cuales poseen un alto nivel de desempeño técnico, con frecuencia pone a la institución en manos de relativamente pocas personas. Esto ha conducido a situaciones donde las empresas se han visto expuestas a chantaje o extorsión.

- **Desaparición de los controles tradicionales**

La importancia de las habilidades técnicas se fortalece con la separación de los controles tradicionales y de las auditorias en muchas instalaciones. La brecha en la comunicación entre el personal técnico, los gerentes de línea y el personal externo, como los auditores antes mencionados, suele causar dificultades para formular las implicaciones practicas de este desarrollo en los términos comerciales convencionales.

La brecha en la comunicación también se extiende a otros expertos como el personal de seguridad. Los gerentes de seguridad rara vez son expertos en computación, por lo que afrontan dificultades al aplicar sus evaluaciones ya establecidas sobre seguridad y riesgo a la actividad de las computadoras.

- **Huelgas, terrorismo urbano e inestabilidad social**

El nivel actual de riesgo en la computación se debe revisar también dentro del contexto de inestabilidad y terrorismo urbanos en muchas partes del mundo. Ha habido ataques físicos a instalaciones en estados unidos y en Europa. Sin embargo, algunas veces se trata de la incursión de personal interno y no de agitadores.

Los ataques internos por parte del personal de una institución pueden tomar la forma de una huelga, esta aunque no sea violenta, puede ser tan perjudicial como el ataque físico.

- **Mayor conciencia de los proveedores**

Hasta hace pocos años este tema no constituía motivo de preocupación para los proveedores, pero la conciencia acerca de la exposición a los riesgos los ha obligado a destinar presupuestos considerables para la investigación sobre la seguridad en computación.

Concepto de seguridad total en computación.

En estos términos, se requiere un enfoque amplio que abarque cierto numero de aspectos relacionados entre si de manera metódica. Hay dos grandes áreas que se deben incorporar a tal enfoque.

1. Aspectos administrativos.
2. Aspectos técnicos y de procedimientos

Los aspectos clave se pueden resumir de la manera siguiente.

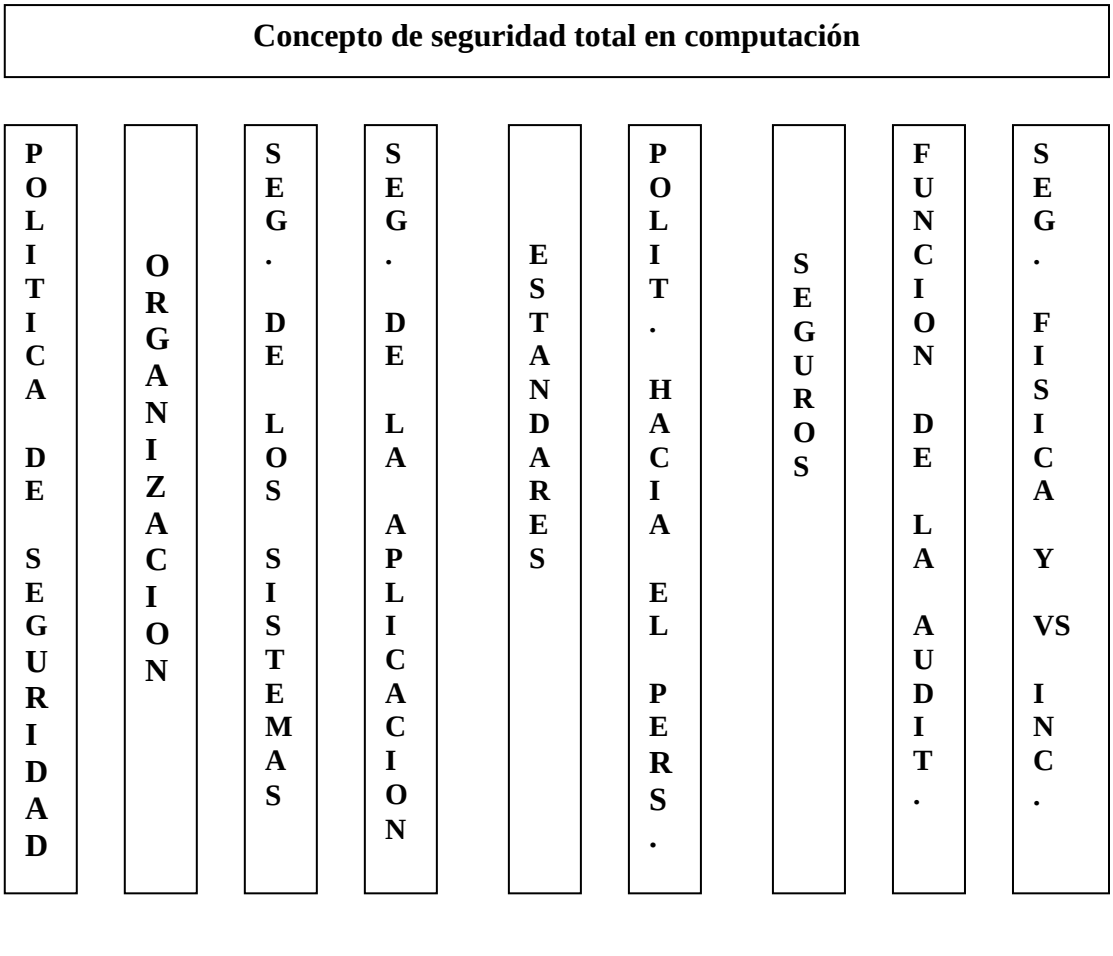
Elementos administrativos.

- Política definida sobre seguridad en computación.
- Organización y división de las responsabilidades
- Seguridad física y contra incendios
- Políticas hacia el personal
- Seguros

Elementos técnicos y de procedimiento.

- Seguridad de los sistemas (equipo y programación, redes y sistemas terminales)
- Seguridad de las aplicaciones, incluyendo la seguridad de los datos y los archivos
- Estándares de programación y operación de los sistemas
- Plan y simulacro para desastres.

Ninguna de estas es por si sola de importancia exclusiva, en una instalación especifica una puede mayor relevancia y por eso requerir mayor atención, sin embargo, si se excluye una de estas áreas se dejarán vacíos en el manejo y control de la seguridad.



Definición de una política de seguridad en computación.

Limitaciones de la seguridad la seguridada depende en última instancia, de la integridad de los individuos que conforman una institución. No existe una seguridad total y cada institución depende de su personal para lograr los niveles de seguridad requeridos.

Equilibrio entre las medidas de seguridad y los niveles de riesgo.

No todas las instalaciones de computación tienen las mismas exigencias de seguridad, algunas son mayores que otras. Cuando se establece el grado de riesgo es importante considerar primero los tipos de riesgos a los que están expuestas las instalaciones de computación:

- Accidentes causados por el mal manejo o negligencia.
- Ataques deliberados en forma de robo, fraude, sabotaje o huelgas.

Cuantificación de los riesgos para la seguridad en computación.

La cuantificación de los riesgos para la seguridad en las computadoras es quizá, la parte más importante del método que una institución adopte sobre la seguridad en computación. A menos que se cuantifiquen los riesgos, será difícil justificar después las medidas identificadas como necesarias.

La cuantificación de los riesgos de seguridad implica ciertos pasos:

1. Clasificación general de las instalaciones en términos de riesgo alto, medio y bajo.
2. Identificación de las aplicaciones que constituyen riesgos altos.
3. Cuantificación del impacto producido por la suspensión prolongada del procesamiento en las aplicaciones de alto riesgo.
4. Formulación de las medidas necesarias para lograr un nivel de seguridad adecuado, es decir, en equilibrio con los niveles de riesgo.
5. Justificación de las medidas de seguridad en cuanto al costo que representan.

Clasificación general de las Instalaciones.

El primer paso consiste en establecer en términos generales si se trata de una instalación de riesgo alto, medio o bajo. Las instalaciones de riesgo alto tienen las características siguientes:

1. Datos o programas que contienen información confidencial de interés nacional o que poseen un valor competitivo alto en el mercado.
2. Pérdida financiera potencial considerable para la comunidad a causa de un desastre o de un gran impacto sobre los miembros del público.
3. Pérdida potencial considerable para la institución y, en consecuencia, una amenaza potencial alta para su subsistencia.

Las aplicaciones de riesgo medio son aquellas cuya interrupción prolongada causa grandes inconvenientes y posiblemente el incremento de los costos, sin embargo, se obtiene poca pérdida material.

Las aplicaciones de bajo riesgo son aquellas cuyo procesamiento retardado tiene poco impacto material en la institución en términos de costo o de reposición del servicio interrumpido.

Al asignar, por ejemplo, 100 puntos a todos los aspectos del inventario y luego clasificar las necesidades de seguridad en términos de riesgo alto, medio y bajo para cada elemento, se deriva la ubicación subjetiva de puntos para cada elemento del inventario. En el nivel de 100 puntos, se tiene una instalación de alta seguridad. La mayoría de los bancos o empresas grandes que dependen en alto grado de sus computadoras se clasifican en un nivel de 90 a 95. La mayor parte de las instalaciones comerciales se encuentran dentro de la escala en un nivel aproximado de 60 a 75.

Identificación de las aplicaciones de riesgo alto, medio y bajo.

Fase uno: elaboración de una lista de aplicaciones por orden de riesgo.
Todas las aplicaciones se deben arreglar en forma tabular y en orden descendente de acuerdo con la importancia del riesgo. Se deben anotar los siguientes datos en cada aplicación:

a) Título o descripción de la aplicación.
b) Programas clave y naturaleza del riesgo, es decir,
    - Aspectos secretos o de interés nacional.
    - Valor competitivo en el mercado debido al carácter único de los aspectos computacionales o a su escala y complejidad.
c) Información de los archivos, también de esta manera:
    - Aspectos secretos o de interés nacional.
    - Confidencialidad interna o valor de mercado.
    - Nivel de riesgo (alto, medio y bajo) y una evaluación general sobre las consecuencias en caso de abuso o desastre.

Al recabar esa información en forma tabular, se facilita la discusión preliminar sobre riesgos a nivel gerencial.

Fase dos: cuantificación del riesgo.
Paso extremadamente difícil y que requiere persistencia. La experiencia indica que el método más práctico para resolver el problema es comenzar por entrevistar a todos lo gerentes directamente afectados por una suspensión en el procesamiento y pedirles que cuantifiquen el impacto causado por la situación. Las respuestas iniciales tal vez varíen en gran medida. Algunos mencionarán pérdidas mínimas debido a procedimiento de apoyo manuales y pérdidas altas. Pero cuando los gerentes comienzan a emitir juicios como “Creo que es un gran riesgo”, se les debe pedir que indiquen con más claridad lo que quieren decir con esa frase.

Fase 3: obtención del consenso sobre los niveles de riesgo.
Este paso es indispensable para lograr el compromiso de la gerencia con el nivel de riesgo definido. Se debe programar una reunión de gerentes que corresponda, en la cual se informa sobre las expresiones sobre riesgos debidamente tabuladas, según se definieron. El propósito de la reunión será lograr el consenso sobre los niveles de riesgo, que por lo general se presentan como rangos más que como cifras absolutas.

Evaluación de las medidas de seguridad.

En esta etapa de revisión preliminar de la seguridad en computación, no es posible obtener todas las recomendaciones detalladas. Esto solo se logrará una vez que se lleve a cabo la revisión a fondo de la seguridad en computación. Sin embargo, es posible definir la estrategia global que se debe seguir para afrontar los niveles de riesgo definidos. Esta estrategia incluye:

1. Aplicaciones, programas y archivos específicos.
2. Planes de detección y métodos para prevenir abusos o desastres.
3. Prioridades, o sea, acciones que se requieren a corto plazo y los elementos que se deben considerar de manera detallada a mediano y largo plazos.

Justificación de las medidas de seguridad en cuanto al costo.

Los pasos seguidos hasta ahora conducen en forma natural hacia la recolección y la presentación de todos los informes necesarios para una decisión bien fundada sobre los costos y los beneficios de la estrategia de seguridad en computación. Toda la información que se obtenga y las decisiones que se tomen se deben documentar de manera progresiva y esto se puede consolidar en el informe final ante la gerencia.

El logro del compromiso con la política de seguridad

Se ha mencionado en varias ocasiones la necesidad de consultar y comprometer a la gerencia pues esta será, en ultima instancia, quien tome la decisión final sobre el método que se adopta y los niveles de gastos. A menos que la gerencia haya participado en las fases anteriores, en improbable que se comprometa por completo con las decisiones que se adoptan. Esta falta de compromiso solo se podrá identificar un poco después de que se realicen en detalle muchas de las medidas recomendadas. El primer problema consiste en determinar quien tiene la responsabilidad general de la seguridad en computación.

Muchos gerentes de línea se dirigen a los gerentes de procesamiento de datos mientras estos difícilmente aceptan la responsabilidad de la seguridad en los departamentos usuarios. Existen dos áreas que se necesitan diferenciar:

1. Asuntos de riesgo comercial.
2. Asuntos de riesgo técnico de las computadoras.

Los asuntos de riesgo comercial son finalmente responsabilidad de la gerencia de línea. Después de un análisis final es difícil que se eluda esta responsabilidad. Los asuntos técnicos son, de manera evidente, responsabilidad de la gerencia de procesamiento de datos. Este es un modo práctico de deslindar responsabilidades, pero se requiere cierta coordinación para garantizar un intercambio productivo entre las funciones comercial y técnica.