1st Peruvian Workshop on IT Security
29.Dic.2003

Calidad y Seguridad en las Tecnologías de la Información

Colaboración

http://escert.upc.es

Instituto de Investigación UNI -FIIS
http://www.uni.edu.pe

Roger Carhuatocto

Miembro esCERT-UPC
Responsable de Servicios Educacionales

esCERT-UPC
C/ Jordi Girona, 1-3. Campus Nord, UPC
08034 Barcelona ~ España
Tel. (34)934015795 ~ Fax. (34)934017055

Inseguridad

- De dónde surgen los problemas?
  - MS?
  - Linux?
  - Open Source/Free Software?
  - Del afán comercial?
  - Usuarios no conocen de tecnologías, el jefe tampoco, quién lo conoce?
  - ... si nadie sabe, para qué se ha comprado?

http://www.santatecla.org
http://www.karsoncomputers.com/stecla

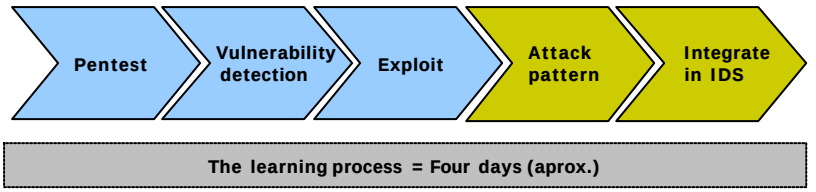
Inseguridad

¿Hay problemas de seguridad? .... sí...

- Ver estadísticas
- Hay roductos deficientes
- Indiferencia, conciencia, educación... desconocimiento..
- Implicación económica, ROI, ROSI...
- Normativa relacionada a TI, Privacidad, comercio electrónico, delitos ...
- "Mundo on-line"

  Crackers, Script Kiddies, Cyberterrorists, exempleados furiosos. Ellos están fuera listos para corromper, interrumpir, robar o sabotear. Quién protege nuestros datos, nuestros sistemas, nuestro negocio de ellos?. Sólo nosotros mismos, pero antes hay que prepararnos.
- Seguridad Reactiva antes que preventiva

PRODUCTOS DEFICIENTES



- Vendedores no consideran a la seguridad seriamente porque no hay incentivo económico, el no aplicar seguridad tampoco les perjudica..

PRODUCTOS DEFICIENTES

- "Computer magazines" comparan la seguridad de sus productos listando sus características, no evaluando su seguridad.
- Ejemplo "Slogans"

PKI Companies and their Slogans [Crypto-Gram Newsletter - October 15, 1999]

I find this amusing. Here are the major, and minor, PKI companies and their corporate slogans. People were paid lots of money to come up with these slogans, so be suitably impressed.

ABAecom: Facilitating electronic banking and commerce over the internet
Baltimore Technologies: Global e-security
CertCo: At the root of electronic commerce
Digital Signature Trust: Creating trust in electronic commerce
Entrust: We bring trust to e-business
GTE Cybertrust: The security to be strategic
Indentrus: Trust on line
IBM/Lotus: Locate, Connect, Secure
Lockstar: Linking legacy to the future
Shym: Unlocking the power of public key
Thawte: <They don't have a slogan, but they have a mission statement in verse.>
Valicert: Enabling global private trust
Verisign: The sign of trust on the net
Xcert: Building trust on the internet

PRODUCTOS DEFICIENTES

- Otro ejemplo: Buscar vulnerabilidades por marca:
  - http://neworder.box.sk/search.php3?srch=verisign

Searching the exploits: (limit 30 results)
(searching titles and full texts)

03.09.2002 : Outlook S/MIME Certificate Chain Vulnerability
11.08.2002 : Internet Explorer SSL Vulnerability
06.08.2002 : Internet Explorer SSL Vulnerability
28.06.2002 : Falsifying a VeriSign Seal (Japan)
09.01.2002 : VeriSign "PayFlow Link" Payment Service Security Vulnerability
25.12.2001 : Internet Explore HTTPS Certificate Attack
20.12.2001 : Trust Issues with RH and Debian Package Managers
10.07.2001 : Many WAP Gateways Do Not Properly Check SSL Certificates
22.03.2001 : Attackers Managed to Obtain Microsoft Digital Signing Keys
23.10.2000 : Using Akamai hosts to circumvent SSL server authentication

PRODUCTOS DEFICIENTES

- Hasta los producto bajo la filosofía “open source” no se salvan: http://www.theregister.co.uk/content/55/27934.html
- Lo bueno es su rápida solución apoyado por la comunidad.

PRODUCTOS DEFICIENTES

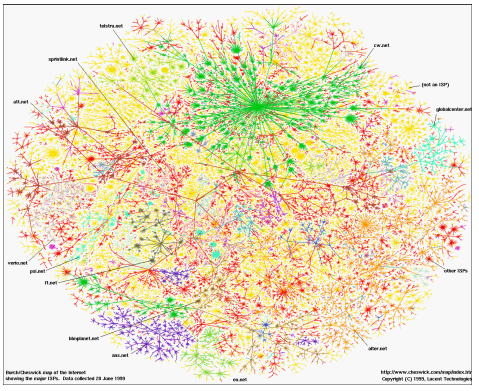
- No hay ley en contra de los proveedores de software de mala calidad, pero hay casos: http://www.wired.com/news/print/0,1294,48980,00.html

PRODUCTOS DEFICIENTES

- Acciones a tomar:
  - ✓ Partial disclosure: CERT, foros, investigadores
  - Qué hacer para que esto no vuelva a pasar?
    - Exigir productos sólidos: probado, que cumple estándares, garantía.
    - Políticas preventivas.
    - Reporte de incidencias.

MUNDO ON-LINE

- Crecimiento de la "red" http://research.lumeta.com/ches/map/
- Fomento a usar internet
  - Declaración de la renta
  - Home banking
  - Compras on-line
  - Administración pública on-line



INDIFERENCIA, CONCIENCIA, EDUCACIÓN

- No se le da la importancia debida a la seguridad
  - Vendedores: aplicar seguridad a los productos no es rentable.
  - Técnicos: menos del 10% de los proyectos IT corresponde a seguridad.
  - Usuarios: desconocimiento, desconocen el verdadero riesgo.
- La seguridad no es un producto, sino un proceso (Bruce Schneier). Se pone mucho énfasis en la capacidad de la tecnología, los productos solos no solucionan el problema.
- Se busca controlar o evitar el riesgo a través de una buena práctica de la seguridad, los productos ayudan.
- Cybersecurity Skills: http://cybersecurity.jrc.es
- eAware: http://www.eaware.org

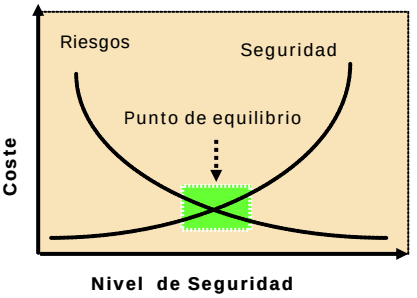
IMPLICANCIA ECONÓMICA

- Internet es un espejo de la sociedad:
  - Fraudes
  - Robo de información, dinero
  - Ataques a servicios
  - .. pérdida de productividad a causa de incidentes de seguridad.
- El riesgo directo es real, hay pérdidas económicas:
  - http://nsi.org/Marketplace/PRs.html
  - $1.5 Trillion, a causa de virus, gusanos
  - $266 billion, Pérdida de ingreso futuro

CURVA DE SEGURIDAD-RIESGO VS. COSTE

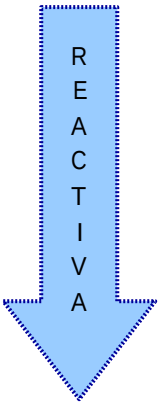
- Costs Versus Benefits in Securing Your Applications
  http://www.scmagazine.com/scmagazine/sc-online/2002/article/50/article.html
- Se busca controlar el riesgo y minimizarlo
  http://www.infosecnews.com/opinion/2002/09/11_03.htm
- La seguridad al 100% es utópica
- Es también importante el riego indirecto: pérdida de clientes, daño a marca, pérdida de la confianza

  - Año 2000, Egghead.com – robo de 1millón de números de tarjetas de crédito
  - CD Universe sufrió el robo de números de tarjetas de créditos, él perdió sus clientes y se fueron a Amazon.com y CDNow
  - Octubre 2000, Microsoft gasta más dinero y esfuerzo manteniendo a relaciones públicas que solucionando problemas de seguridad. La percepción pública es que el código fuente no fue contaminado fue más importante que los efectos del actual ataque.



CÓMO ERA LA SEGURIDAD?

- 1980, Seguridad tradicional
  - Simple: no se escuchaba de DOS, ataques a web servers, fallas en el lenguaje de scripts para web server, vulnerabilidades del outlook... Sólo antivirus
- Aparecen los firewalls
- Aparecen los primeros IDS
- Últimos años, VPN, PKI, SmartCards, biométricos
- Nuevos servicios, nueva “windows exposure”: wireless
- Nuevos requerimientos: privacidad, seguros, piratería, ...



PERSPECTIVAS

- Insurance and the Future of Network Security - http://www.schneier.com/crypto-gram-0103.html#3
  - Digital Forensics lleva ventaja
  - Faltan que las aseguradoras emprendan esta actividad
- Privacidad: tecnologías para salvaguardar la privacidad
  - Criptografía
- Cambiar o morir:
  - Firewalls
    - Unicode, Tráfico viene de muchos puntos, wireless?, Redes muy rápidas, se convierte en cuello de botella
  - IDSs:
    - Muchos falso positivos, analizar el tráfico es el problema, El tráfico viene cifrado (ipsec), Tráfico no viene solamente de un lugar, Considera redes wireless?, Redes muy rápidas - se convierte en cuello de botella, el objetivo es reaccionar o prevenir? (Intrusion Prevention System)

Calidad y Seguridad

"Para gestionar la calidad hace falta asegurar todo el ámbito de los Sistema de Información de la empresa."

Ámbitos de los Sistemas de Información

- Infraestructura.
- Software.
- Información.
- Personal.
- Prestación del Servicio.
- Gestión.

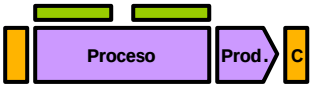
Gestión de la Calidad: Evolución I

1. **Inspección**
   - Separación después de la producción de los productos defectuosos de los no defectuosos.
   - Buscar la ausencia de defectos.
   - Auditoria final, reuniones para solucionar defectos.

2. **Control de Proceso**
   - Anticipación dentro de los procesos de desarrollo.
   - No se espera al final de la cadena de producción.
   - Se introduce el concepto de proceso.

3. **Gestión Integral de la Calidad**
   - la Calidad debe abarcar a todas las áreas de las empresa que intervienen en la realización del producto.

4. **Calidad Total**
   - Forma de gestión de una organización centrada en la calidad basada en la participación de todos sus miembros y que apunta al existo a largo plazo por medio de la satisfacción del cliente y a proporcionar beneficios para todos los miembros de la organización y para la sociedad.



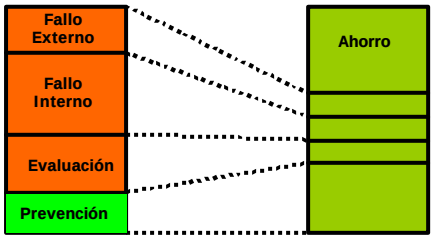
Modelos Calidad: Testing

- **Es "Testing" calidad?**
  - Análisis de vulnerabilidades
  - Penetration Testing
- Seguimos pensando en que es problema del producto final?

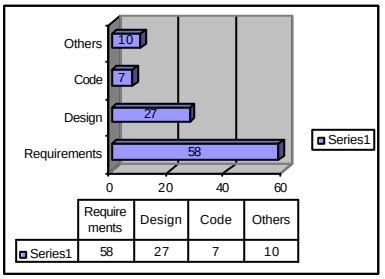
- ISO 9126 - Evaluación y control del calidad de software y producto final
- ISO 9001 - Proceso de como desarrollar el producto
- ISO 17799 – Best practices in information security

  - Testing es un apoyo para controlar
  - OSSTMM es una guia que nos asiste en Test de Servicios(http, ftp, etc..) desde fuera (Internet)

Calidad IT: Nuestra metodología I



El retorno de la inversión en calidad, vendrá determinado por la velocidad de disminución de los costes Externos, Internos y de Evaluación



Fuente: Software testing in the Real World

El origen de defectos en el productos está en los "requisitos"

Predicting the Future of Testing
http://www.stickyminds.com/pop_print.asp?ObjectId=6887&ObjectType=COL

Calidad IT: Nuestra metodología II

1. Familia ISO 9000: ISO 9001, 9002 y 9003 (Certificables)

- **ISO 9001**, Modelo de Certificación de la Calidad en diseño, desarrollo, producción, instalación y servicios. Es fundamental para demostrar en el mercado la calidad total del servicio desde producción a post venta. Anula y reemplaza la segunda edición (ISO 9001:1994), así como a las Normas ISO 9002:1994 e ISO 9003:1994
- **ISO 9002**, Modelo para Certificación de Calidad en producción, instalación y servicios. Es el requerimiento de standard cuando una empresa no es responsable del diseño y desarrollo del producto o servicios, pero aspira a demostrar excelencia para producción, instalación y servicios (es idéntica a la ISO 9001 excepto por el requerimiento de control del diseño.
- **ISO 9003**, Modelo para certificación de Calidad en Inspecciones y tests finales. Es el requerimiento de standard que usa una empresa para demostrar excelencia para controlar sus productos por inspecciones y tests finales.

Calidad IT: Nuestra metodología III

2. Guías y directrices

ISO 9000: Normas para la Gestión de la Calidad y Aseguramiento de Calidad. Reglas generales para su selección y utilización.

- ISO 9000/1: Directrices para la selección y uso de Normas.
- ISO 9000/2: Reglas generales para la aplicación de las normas.
- ISO 9000/3: Guía para la aplicación de ISO 9001 al desarrollo, suministro y mantenimiento del soporte lógico.
- ISO 9000/4: Aplicación para la gestión de la seguridad de funcionamiento.

ISO 9004: Gestión de la Calidad y elementos de un Sistema de Calidad. Reglas generales.(Mejora de desempeño)

- ISO 9004-1: Parte 1: Directrices.
- ISO 9004-2: Parte 2: Guía para los Servicios.
- ISO 9004-3: Parte 3: Guía para materiales procesados.
- ISO 9004-4: Parte 3: Guía para la Mejora de la Calidad.
- ISO 9004-5: Guía para la preparación de Planes de Calidad.

ISO 10011: Reglas generales para la Auditoria de los Sistemas de Calidad.

- ISO 10011-1: Parte 1: Auditorias.
- ISO 10011-2: Criterios de cualificación de los auditores de los Sistemas de la Calidad.
- ISO 10011-3: Gestión de los programas de auditoria

ISOs: http://www.aunmas.com/guias/iso/publicaciones.htm
Ejem. reales ISOs: http://www.aunmas.com/guias/iso/ejemplos.htm

Calidad IT: Nuestra metodología IV

3. Estándares para SW

- Data Structure-Oriented design
- Object-Oriented design
- Prototyping
- Modelo de McCall et al. (1977) o FCM (Factor Criteria Metric) model
  http://www.dcs.qmul.ac.uk/~norman/papers/qa_metrics_article/section_3_metrics.html
- SDLC Model versión x – The waterfall model / System Development Lifecycle
  http://www.abdn.ac.uk/~acc025/web_pgs/public/courses/as/other/SDLC/intro2.htm
- ISO 9000-3, Guía para la aplicación de la ISO 9001 al proceso de SW.
- ISO 9126-1, Software Engineering – Product Quality – Part 1: Quality Model
- ISO 14598-1, Information Technology – Evaluation of Software Products – General Guide
- ISO 15408 - Common Criteria (21 Agosto – Versión 2.1)
  http://csrc.nist.gov/cc/index.html
- V-Model – Software Lifecycle Process Model (German Process Model)
- Métricas:
  - Los mismo estándares proporcionan modelos para definir métricas
  - Capability Maturity Model for Software (CMM or SW-CMM)
    http://www.sei.cmu.edu/cmm
- Hay muchos: http://www.12207.com

Calidad IT: The New Methodology

4. Agile Software Development ("liviana")

- **Extreme Programming (XP) is actually a deliberate and disciplined approach to software development.**

  http://www.extremeprogramming.org

Manifesto for Agile Software Development

We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:

Individuals and interactions over processes and tools
Working software over comprehensive documentation
Customer collaboration over contract negotiation
Responding to change over following a plan

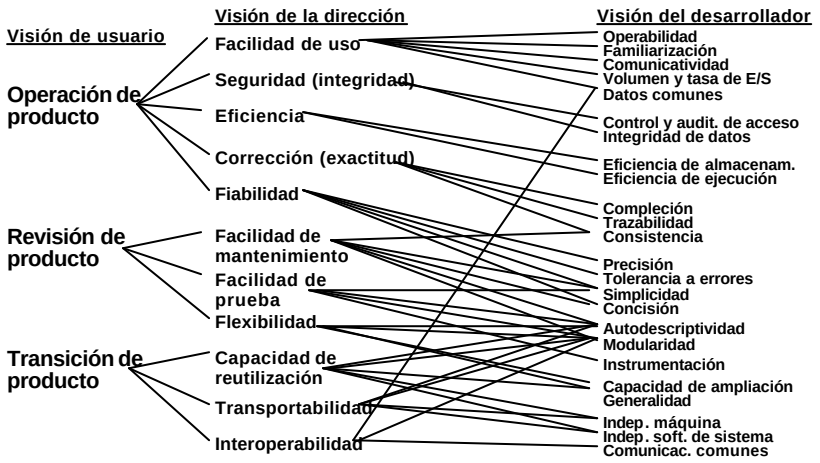
That is, while there is value in the items on the right, we value the items on the left more.

http://www.agilemanifesto.org

The New Methodology:
http://www.martinfowler.com/articles/newMethodology.html
La Nueva metodología:
http://www.programacionextrema.org/articulos/newMethodology.es.html

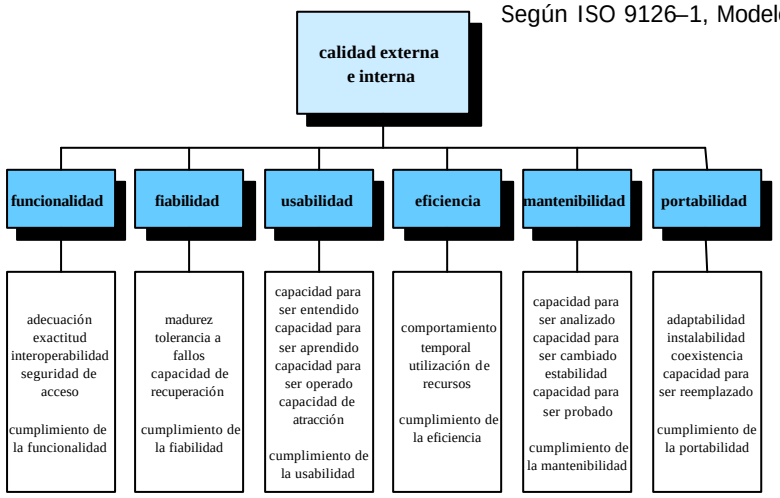
Calidad IT: El criterio I

Según Kim McCall



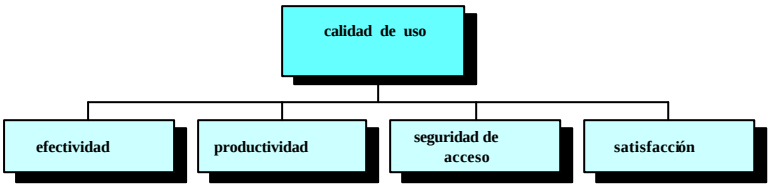
Calidad IT: El criterio II

Según ISO 9126–1, Modelo de Calidad



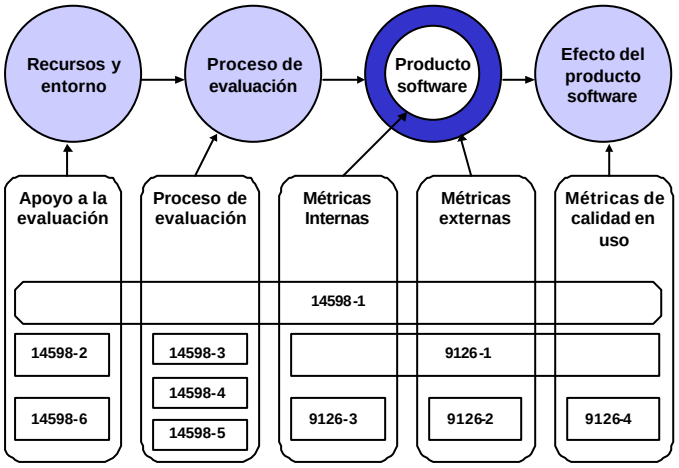
Calidad IT: El criterio II

Según ISO 9126–4, Metricas de Calidad de Uso



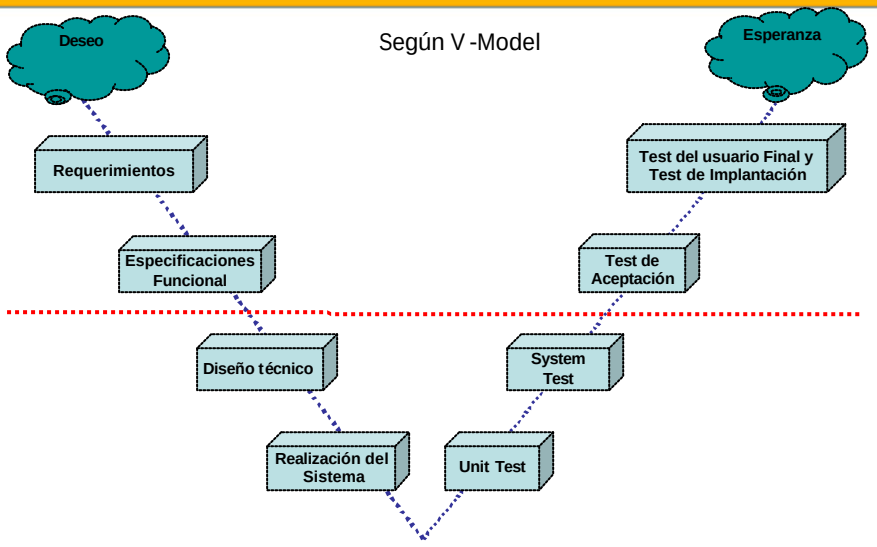
Calidad IT: El criterio III

Según ISO 14598

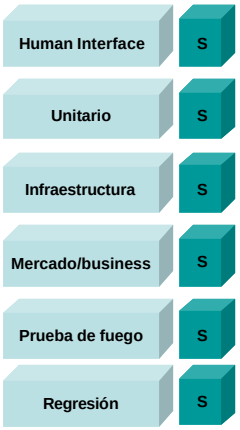


Calidad IT: El criterio IV

Según V-Model



Calidad IT: Testing como medio para ....



Test de usabilidad, GUI, Estándares, Security interface

Test de unitario, Código seguro

Test de Configuración del entorno, Performance testing (S), Test de recuperación (S), Security y Penetration Testing (S), Test de coexistencia

Test de funcionalidad(S), Interfaces entre plataformas (S), Test de final al Extremo (S+), Integridad de data (S+)

Test de implementación, Beta testing, Test de aceptación del cliente/usuario (S), Seguridad interna y externa (S)

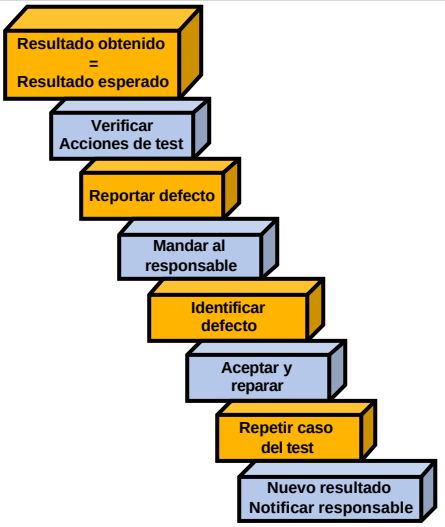
Regression Testing (S+), Sanity/Smoke Testing (S+)

Calidad IT: Sistemas de Gestión: Soporte

- Gestión de versiones
- Gestión de bugs
- Gestión de incidencias
- Gestión de Requerimientos, Test Plan, Test Case
- Herramientas CASE
- Workgroup
- .....

DEFECTOS: Bugs, fix, xploits, workaround, patch..

- Que es un defecto?
El resultado del test obtenido no es igual al resultado que esperaba!
- Cuando reportar?
Siempre



Calidad – Seguridad: conclusiones

CALIDAD y SEGURIDAD

- La seguridad es más que una característica de un producto final
- Seguridad es un proceso, no un producto (no es reactiva, no es intrínseca a un producto, se aplica a todos los elementos que interactúan con el proceso)
- Seguridad al 100% es utópico
- Gestionar el riesgo, buscar el riesgo mínimo
- Outsourced security : La empresa debe dedicarse a su negocio..
- Nuevos escenarios: seguros, privacidad

CALIDAD y SEGURIDAD

- La seguridad es resultado de una baja calidad. Pensar en calidad, la seguridad está implícita
- La calidad se aplicada a todo el proceso de negocio
- En las IT, el enfoque de calidad es el mismo para otro tipo de infraestructura. Es aplicable.
- La seguridad no es “moda”

REFERENCIAS: Seguridad, ensayos

- Costs Versus Benefits in Securing Your Applications
  http://www.scmagazine.com/scmagazine/sc-online/2002/article/50/article.html
- Outsourcing of security
  http://computer.org/computer/sp/articles/sch/index.htm
- The process of security
  http://www.infosecuritymag.com/articles/april00/columns_cryptorhythms.shtml
- Security pitfalls in security
  http://www.counterpane.com/pitfalls.html
- Full disclosure
  http://www.counterpane.com/crypto-gram-0111.html
- Testimony and Statement for the Record of Bruce Schneier
  http://www.counterpane.com/commerce-testimony.html
- The Disclosure Debate
  http://www.infosecuritymag.com/2002/jul/roundtable.shtml
- Managed Security Monitoring vs. Managed Security Services
  http://www.counterpane.com/msm.html
- Boletines:
  - http://www.infosecuritymag.com/
  - http://www.securityfocus.com
  - http://www.scmagazine.com
  - http://www.theregister.co.uk
  - ...

REFERENCIAS: Calidad, testing

www.stickyminds.com/ – Sobre testing
www.webpagesthatsuck.com – Lo que dice
www.csst-technologies.com – Server testing refences
www.w3c.org – Testing, security con mucha informacion
http://www.testingfaqs.org/ - Testers reunidos
www.softpanorama.org/SE/testing.shtml - Testing Site links
www.teamshare.com – Defectos
www.pb-sys.com/ - Download buggit
http://www.testingfaqs.org/t-track.htm - Lista con herramientas Para defectos

- The Real World of Software Testing - http://srkprasad.blogspot.com
- W Edwards Deming - http://www.dti.gov.uk/mbp/bpgt/m9ja00001/m9ja000016. html
- Predicting the Future of Testing
  http://www.stickyminds.com/pop_print.asp?ObjectId=6887&ObjectType=COL