OWASP LatamTour
Chile 2011

The OWASP Foundation
http://www.owasp.org

OWASP TOP10 como base para Inspección de Código

Nombre relator
Katherine Andrade

Katherine.andrade@testgroup.cl

Temario

- Por que la seguridad es un factor crítico de su negocio?
  - Evolución del mercado automotriz
  - Evolución del mercado de transacciones electrónicas
- Riesgos vigentes en el comercio electrónico
- Definición de las fases de maduración
- Como partir.. Donde partir
- Resultados

El mercado automotriz

- **35 años atrás**
  - La mayoría de los coches se construían sin dispositivos seguridad
  - No eran frecuentes airbags, zonas de deformación, protección contra impactos laterales, etc.
- **El mercado, los clientes cambiaron**
  - Mayor acceso a vehiculos familiares
  - Regulaciones más exigentes.
  - Retirar del mercado modelos con fallas

- **La industria incluye más características de seguridad**
  - La seguridad se convierte en un factor crítico de venta
  - Los compradores exigen más "seguridad del producto" como un valor diferenciador.

3

Evolución del mercado electrónico

- El incremento de transacciones electrónicas en el mercado Chileno y mundial, implica también una mayor exposición y riesgo al fraude.
- La penetración de internet masifica la demanda por transacciones electrónicas. Los usuarios de banca electrónica se incrementan.
- El riesgo de fraude afecta al usuario y a la institución que administra y provee los servicios de acceso a banca electrónica y transacciones electrónicas.
- El mayor riesgo (largo plazo) radica en la perdida de confianza de los clientes.

Evolución del mercado electrónico

- **Como prevenir fraudes?**
- **Como asegurar la estabilidad de las aplicaciones comerciales?**
- **Existe una norma que ayude a este objetivo?**

- El PCI Security Standards Council (Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago); es un foro mundial abierto, establecido en 2006, fundado por las marcas: Visa, MasterCard, American Express, Discover Financial Services y JCB International.

- La misión de PCI es aumentar la seguridad de los datos de cuentas de pago y de las aplicaciones de comercio electrónico (asociado a la Industria de tarjetas de pago).

- Las empresas fundadoras han acordado que PCI DSS sea el requisito técnico a cumplir en sus programas de seguridad de información sensible, y es aplicable a todos los actores que intermedian en la transacción electrónica.

Riesgos por no cumplimiento de PCI DSS

- Potencial de robo de identidades de clientes debido a la exposición de la información.
- Revocación del permiso o franquicia de las marcas
- Sanciones económicas impuestas por las marcas de tarjetas de pago:
  - Implicaciones financieras
  - Pérdida de ingresos
  - Posibles demandas

Las marcas de pago podrán, a su discreción, multar a un asociado comercial desde US$ 5.000 a US$ 100.000 por mes para cada evento de incumplimiento del estándar PCI.
(fuente: www.pcicomplianceguide.org)

- Impacto en la imagen y reputación del negocio

Qué medidas sugiere la norma PCI DSS ?

PCI DSS tiene 6 objetivos de control y 12 requisitos de seguridad a cumplir.

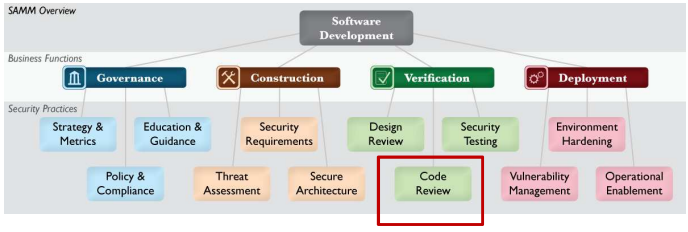
Objetivos de Control	Requisitos de seguridad PCI DSS	
1. Construir y mantener una infraestructura segura	r1: Instalar y mantener una configuración de firewall para prot de tarjetas. r2: No emplear configuraciones por defecto en los elementos	✓ Solución Técnica ✓ Solución Técnica
2. Proteger los datos de los titulares	r3: Proteger los datos almacenados de titulares de tarjeta. r4: Encriptar las transmisiones de datos de titulares de tarjeta	✓ Solución Técnica
3. Mantener un programa de gestión de las vulnerabilidades	r5: Emplear y actualizar periódicamente el software antivirus. r6: Desarrollar y mantener sistemas y aplicaciones seguras.	OWASP
4. Implementar medidas fuertes de control de acceso	r7: Restringir el acceso a los datos de titulares al ámbito de lo para ofrecer el servicio. r8: Asignar un identificador único a cada persona con acceso a equipos de proceso r9: Restringir la seguridad física para acceder a los datos de ti	✓ Solución Técnica ✓ Solución Técnica
5. Monitorizar y someter a pruebas regulares las redes	r10: Monitorizar y hacer seguimiento a todos los recursos de r r11: Probar regularmente la seguridad de los sistemas y proce	✓ Solución Técnica
6. Mantener una Política de Seguridad de la Información	r12: Mantener una política que cubra la seguridad de la informa	✓ Procesos

Desde donde partir? Como?

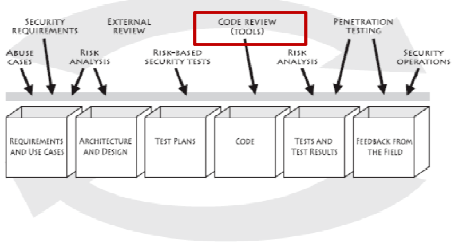
- Inspección de código (Code Review)

OWASP
The Open Web Application Security Project
http://www.owasp.org

PCI Security Standards Council



SOFTWARE SECURITY
BUILDING SECURITY IN



8

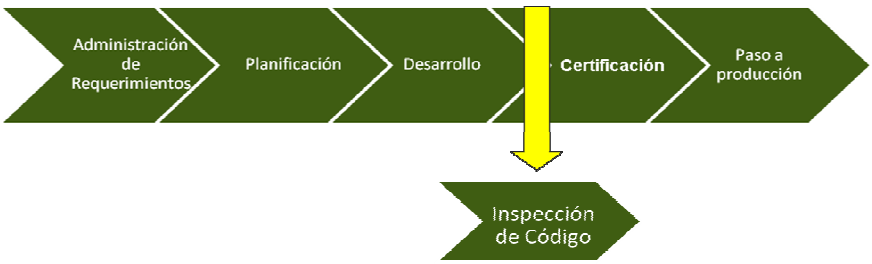
Desde donde partir? Como?

Análisis de Código Estático (Static Code Analysis)

Adherir a normativas y basarse en modelos de referencia, tales como:

- Normativa PCI DSS (Payment Card Industry Data Security Standard)
- Recomendaciones del Code Review de OWASP.
- Estándares de codificación segura del CERT "Secure Coding Standard"

Insertar la práctica en el ciclo de vida del desarrollo



9

Modelo para evolucionar Inspección de Código…

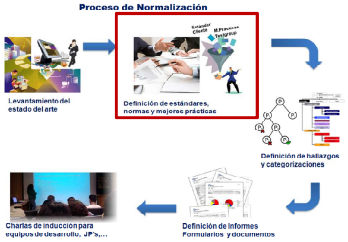
Revisión – Seguridad

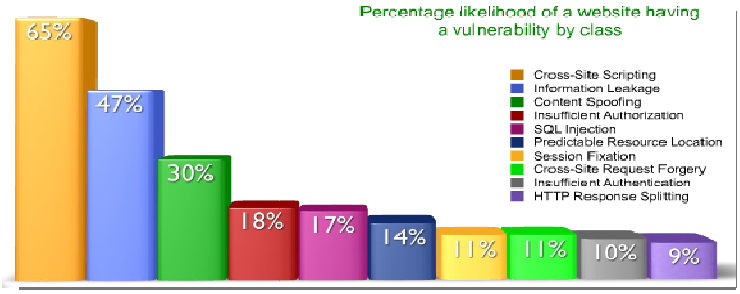
OWASP Top Ten

Enumera y describe los 10 riesgos más críticos en las aplicaciones web.

Se ha vuelto un estándar aceptado por la industria

- **PCI DSS**
- **US Federal Trade Commision (FTC)**
- **US Defense Information Systems Agency (DISA)**

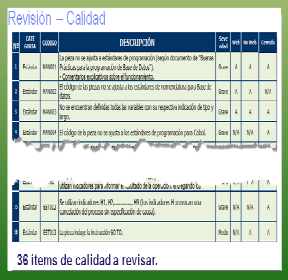


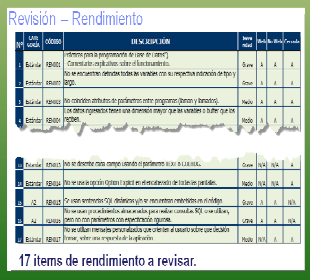


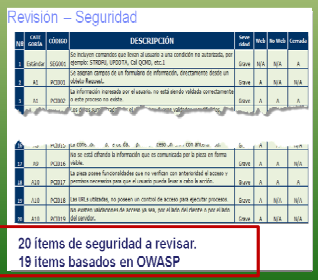
Desde donde partir? Como?

- **Inspección de código (ICOD)**

	Segmentado por Severidad o Gravedad			
Tipificación	**Grave**	**Leve**	**Medio**	**Total general**
Calidad	16	8	12	36
Rendimiento	11	1	5	17
Seguridad	20			20
Total general	**47**	**9**	**17**	**73**





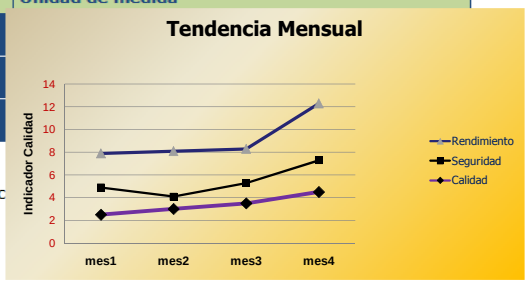


Información de Gestión…

Medición Para el Total de Piezas

Total de Piezas
Cantidad de piezas revisadas.
Cantidad total de defectos detectados por piezas de código.
Cantidad de defectos severidad grave detectados por piezas de código.
Cantidad de defectos severidad media detectados por piezas de código.

Métrica	Unidad de medida
Cantidad total de defectos detectados por piezas de código.	
Cantidad de defectos severidad grave detectados por piezas de código.	
Cantidad de defectos severidad media detectados por piezas de código.	

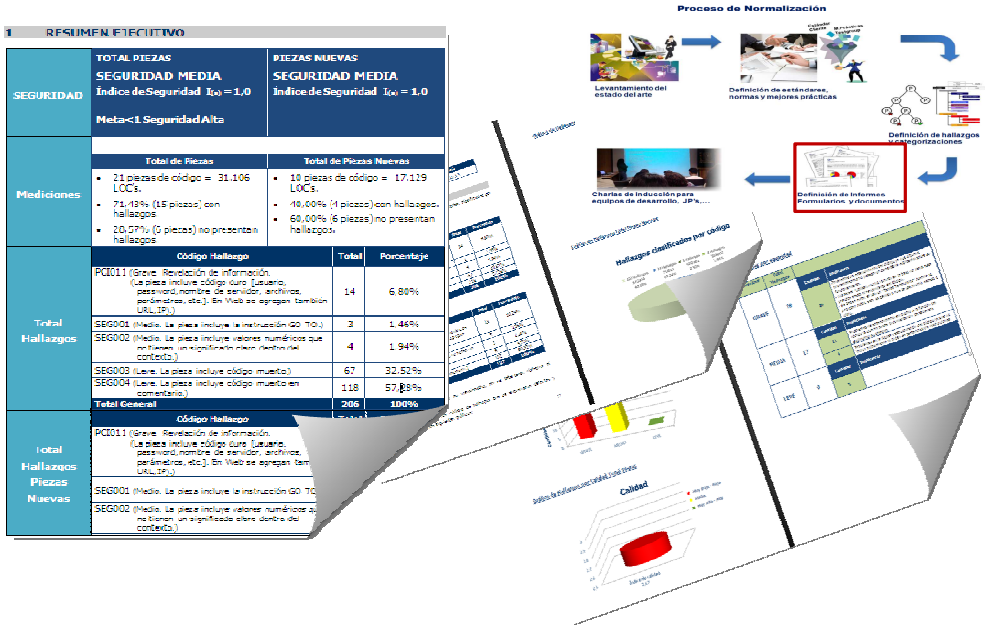


De lo anterior, se calcula el indicador de c

$$I_{(c)} = \frac{\sum_{i=1}^{n} P_i}{n}$$

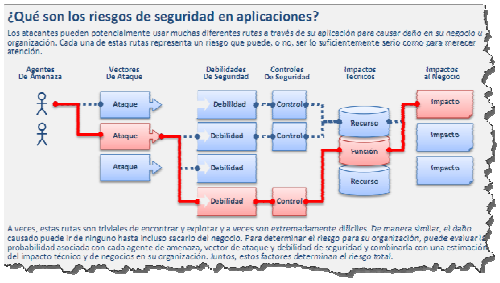
En que "P_i" representa al valor en PESO de la medición realizada para cada una de las métricas y "n" representa el total de métricas.

Información de Gestión: Calidad / Seguridad / Rendimiento



Entrenamiento al personal… Evangelizar…

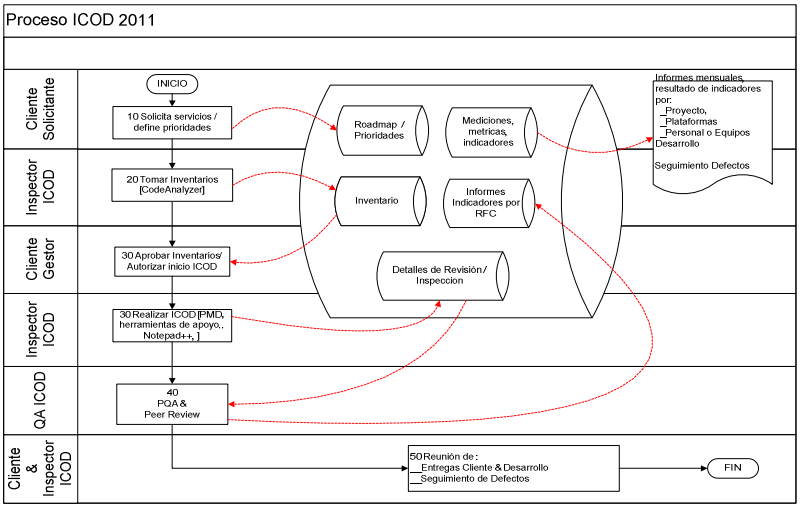
Charlas de inducción para equipos de desarrollo, JP's,…



T10 OWASP Top 10 2010 – Riesgos de Seguridad en Aplicaciones Web

- **A1 – Inyección**: Las fallas de inyección, tales como SQL, OS y LDAP, ocurren cuando datos no confiables son enviados a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al intérprete en ejecutar comandos no intencionados o acceder datos no autorizados.
- **A2 – Secuencia de comandos en sitios cruzados (XSS)**: Las fallas XSS ocurren cada vez que una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada. XSS permite a los atacantes ejecutar secuencia de comandos en el navegador de la víctima los cuales pueden secuestrar las sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso.
- **A3 – Pérdida de Autenticación y Gestión de Sesiones**: Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son frecuentemente implementadas incorrectamente, permitiendo a los atacantes comprometer contraseñas, llaves, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios.
- **A4 – Referencia Directa Insegura a Objetos**: Una referencia directa a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, tal como un fichero, directorio, o base de datos. Sin un chequeo de control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder datos no autorizados.
- **A5 – Falsificación de Peticiones en Sitios Cruzados (CSRF)**: Un ataque CSRF obliga al navegador de una víctima autenticada a enviar una petición HTTP falsificada, incluyendo la sesión del usuario y cualquier otra información de autenticación incluida automáticamente, a una aplicación web vulnerable. Esto permite al atacante forzar al navegador de la víctima para generar pedidos que la aplicación vulnerable piensa son peticiones legítimas provenientes de la víctima.
- **A6 – Defectuosa configuración de seguridad**: Una buena seguridad requiere tener definida e implementada una configuración segura para la aplicación, marcos de trabajo, servidor de aplicación, servidor web, base de datos, y plataforma. Todas estas configuraciones deben ser definidas, implementadas, y mantenidas ya que por lo general no son seguras por defecto. Esto incluye mantener todo el software actualizado, incluidas las librerías de código utilizadas por la aplicación.
- **A7 – Almacenamiento Criptográfico Inseguro**: Muchas aplicaciones web no protegen adecuadamente los datos sensibles, tales como tarjetas de crédito, SSSs, y credenciales de autenticación con mecanismos de cifrado o hashing. Atacantes pueden modificar o robar tales datos protegidos inadecuadamente para conducir robos de identidad, fraudes de tarjeta de crédito u otros crímenes.
- **A8 - Falla de Restricción de Acceso a URL**: Muchas aplicaciones web verifican los privilegios de acceso a URLs antes de generar enlaces o botones protegidos. Sin embargo, las aplicaciones necesitan realizar controles similares cada vez que estas páginas son accedidas, o los atacantes podrán falsificar URLs para acceder a estas páginas igualmente.
- **A9 – Protección Insuficiente en la capa de Transporte**: Las aplicaciones frecuentemente fallan al autenticar, cifrar, y proteger la confidencialidad e integridad de tráfico de red sensible. Cuando esto ocurre, es debido a la utilización de algoritmos débiles, certificados expirados, inválidos, o sencillamente no utilizados correctamente.
- **A10 – Redirecciones y Reenvíos no validados**: Las aplicaciones web frecuentemente redirigen y reenvían a los usuarios hacia otras páginas o sitios web, y utilizan datos no confiables para determinar la página de destino. Sin una validación apropiada, los atacantes pueden redirigir a las víctimas hacia sitios de phishing o malware, o utilizar reenvíos para acceder páginas no autorizadas.

Ahora por fin podemos iniciar … la inspección



Servicio de Inspección de Código… en régimen

El **IcodManager** recibe una Solicitud de Inspección y la incorpora al Roadmap.

El **IcodManager** a partir del Roadmap, actualiza el calendario de inspecciones.

El **IcodManager** presenta Calendario de Inspecciones a su contraparte para aprobar/modificar secuencias/prioridad.

El **Inspector de Código**
_Inspecciona las Piezas de sw
_Emite informes de resultados
_Envía informes a T.Manager

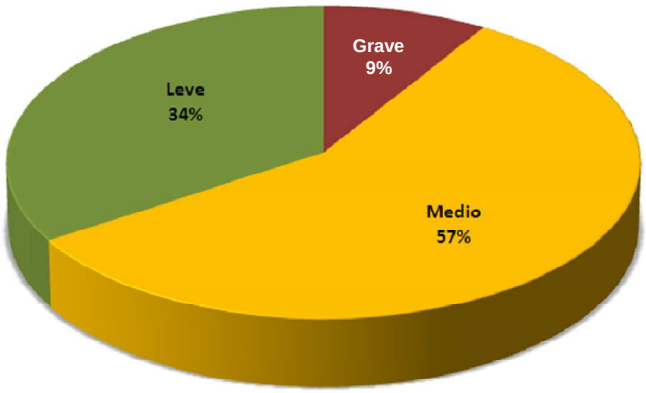
El IcodManager:
_Supervisa desempeño de Equipo
_Revisa/Corrige informes de Inspección
_Envía entregable al Cliente.

Y los resultados…

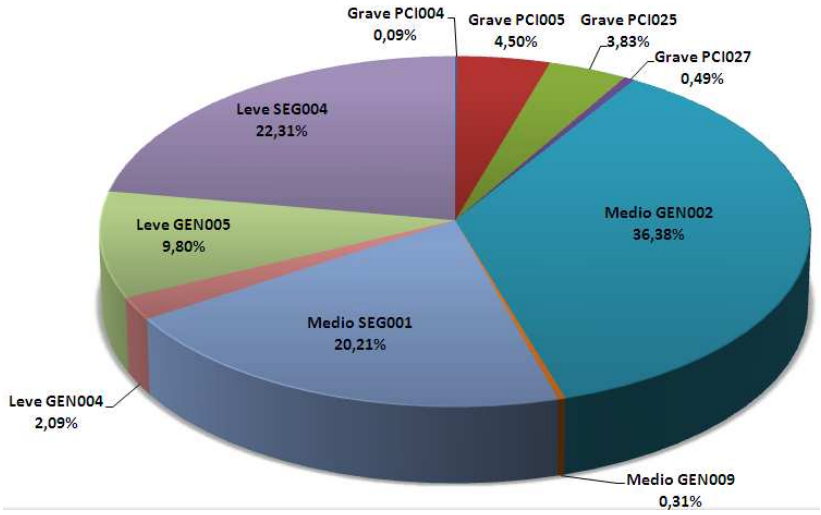
"MÁS DE 5 MILLONES DE LINEAS DE CÓDIGO INSPECCIONADAS"

(JAVA, COBOL, RPG, SQL, C, C++, VISUALBASIC, .NET)

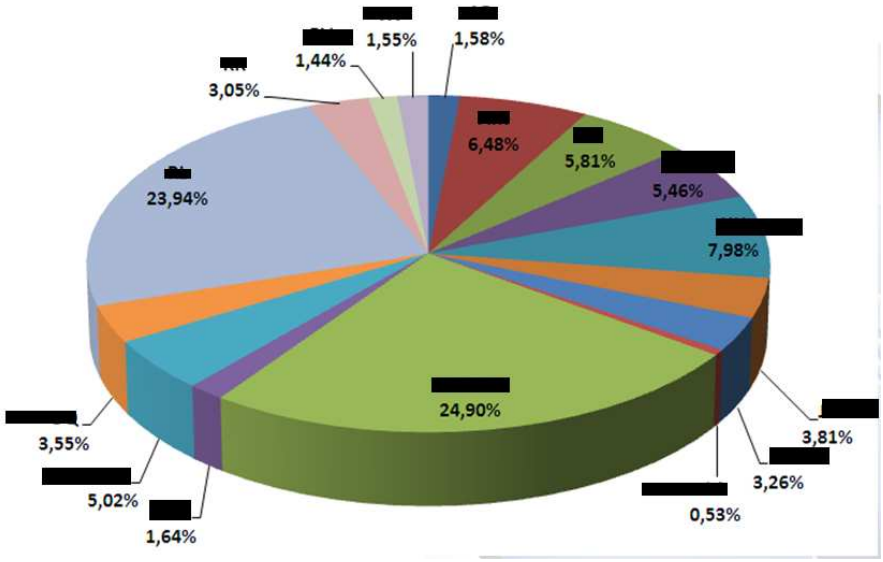
Hallazgos por Severidad



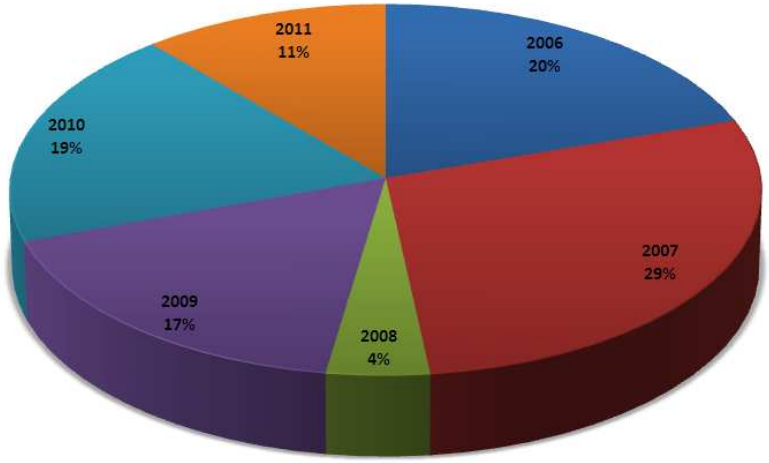
Hallazgos Severidad v/s Código



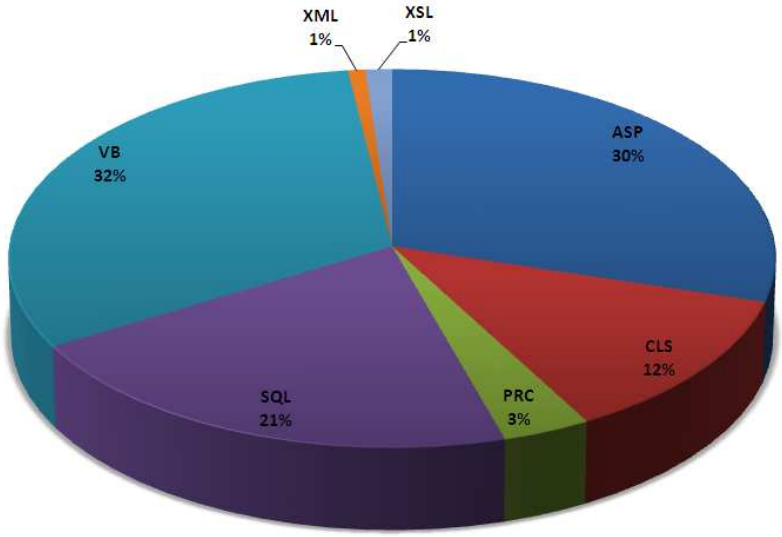
Hallazgos por Equipo Desarrollo



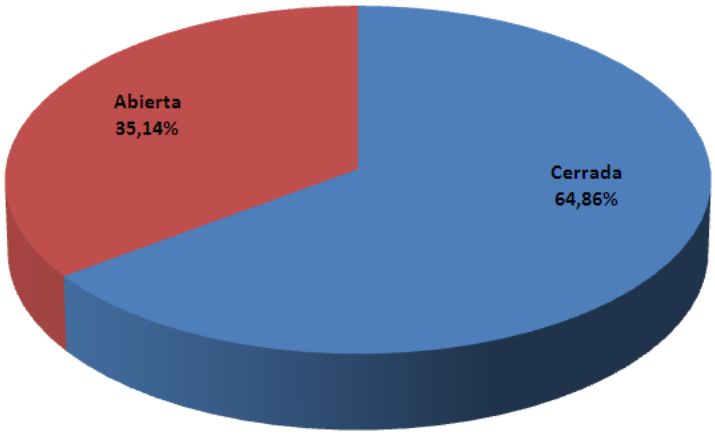
Hallazgos por año



Hallazgos por tipo de código



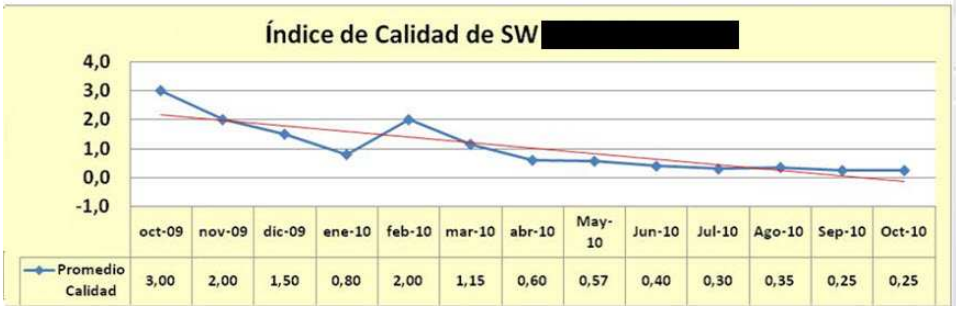
Hallazgos por plataforma



24

Índicadores y Tendencias

	oct-09	nov-09	dic-09	ene-10	feb-10	mar-10	abr-10	May-10	Jun-10	Jul-10	Ago-10	Sep-10	Oct-10
Promedio Seguridad	1,00	1,50	1,30	2,00	1,00	0,80	0,33	0,72	0,43	0,45	0,55	0,50	0,53



	oct-09	nov-09	dic-09	ene-10	feb-10	mar-10	abr-10	May-10	Jun-10	Jul-10	Ago-10	Sep-10	Oct-10
Promedio Calidad	3,00	2,00	1,50	0,80	2,00	1,15	0,60	0,57	0,40	0,30	0,35	0,25	0,25

25

Y como se paga la inspección de código?

Costos aplicando Inspección de Código

Etapa de la detección de los defectos	Cantidad de defectos latentes	Defectos identificados	US$ Costo por corregir cada defecto detectado	Total US$ por corregir
Después del desarrollo	463			
Después de ICOD	180	283	25	$ 7.075
Después del Testing Funcional	113	67	200	$ 13.400
Después de UAT/Producción	32	81	1000	$ 81.000
Total US$				**$ 101.475**

Costos SIN aplicar Inspección de Código

Etapa de la detección de los defectos	Cantidad de defectos latentes	Defectos identificados	US$ Costo por corregir cada defecto detectado	Total US$ por corregir
Después del desarrollo	463			
~~**Después de ICOD**~~			~~25~~	
Después del Testing Funcional	321	142	200	$ 28.400
Después de UAT/Producción	124	197	1000	$ 197.000
Total US$				**$ 225.400**

Ref.: www.smartbear.com

Preguntas