Maestría en Seguridad Informática

Construcción de seguridad en metodologías Ágiles

Jorge Ezequiel, Bo
Hugo Pagola
Alberto Dums

Agenda

1. Introducción
2. Metodologías Ágiles
3. Problema de estudio
4. Experimentación
5. Conclusiones

¿Qué entendemos?

- Legislaciones
- G. Riesgos
- G. Incidentes

- Criptografía
- G. Identidad
- C. Acceso
- Firma Digital

- Firewalls
- IDS

Mecanismos de seguridad

Funcionalidades de seguridad
VS.
Funcionalidades seguras

Hechos recientes de problemas de seguridad

NEWS

Latest SQL Injection Campaign Infects 1 Million Web Pages

Brecha de seguridad encontrada en el sitio web de MasterCard por NullCrew

Publicado en 1 octubre, 2012 por Sigma en Google, Internet, Noticias, Seguridad

Un grupo de hackers conocido como NullCrew Scripting (XSS) en el sitio web oficial de Mas resulto ser vulnerable a un ataque de XSS.

Vulnerabilidad XSS en PayPal.com

PUBLICADO POR VICENTE MOTOS ON LUNES, 27 DE MAYO DE 2013 ETIQUETAS: VULNERABILIDADES, XSS

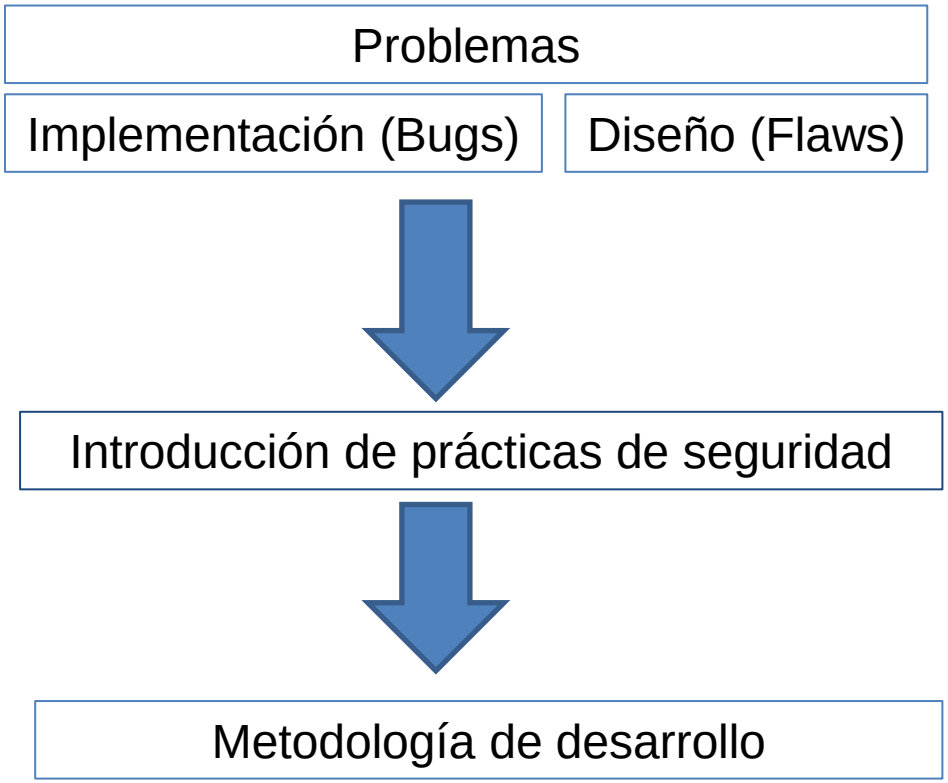
Leyendo las listas de Full disclosure llama la atención una **vulnerabilidad XSS (Cross-Site Scripting) que todavía sigue presente en la web de búsqueda de PayPal:**

Falla de seguridad en Faceb teléfono de los usuarios

Publicado en 8 octubre, 2012 por Sigma en Facebook, Noticias, Seguridad, Tecnologias

Suriya Prakash, un **investigador de seguridad** de la India ha descubierto **una falla de seguridad grave en Facebook** que permite a los **delincuentes informáticos (no hackers)** obtener los números telefónicos de millones de usuarios de esta **plataforma tecnológica.**

¿Como construir funcionalidades seguras?



Metodologías de desarrollo

¿Tradicional o Ágil ?

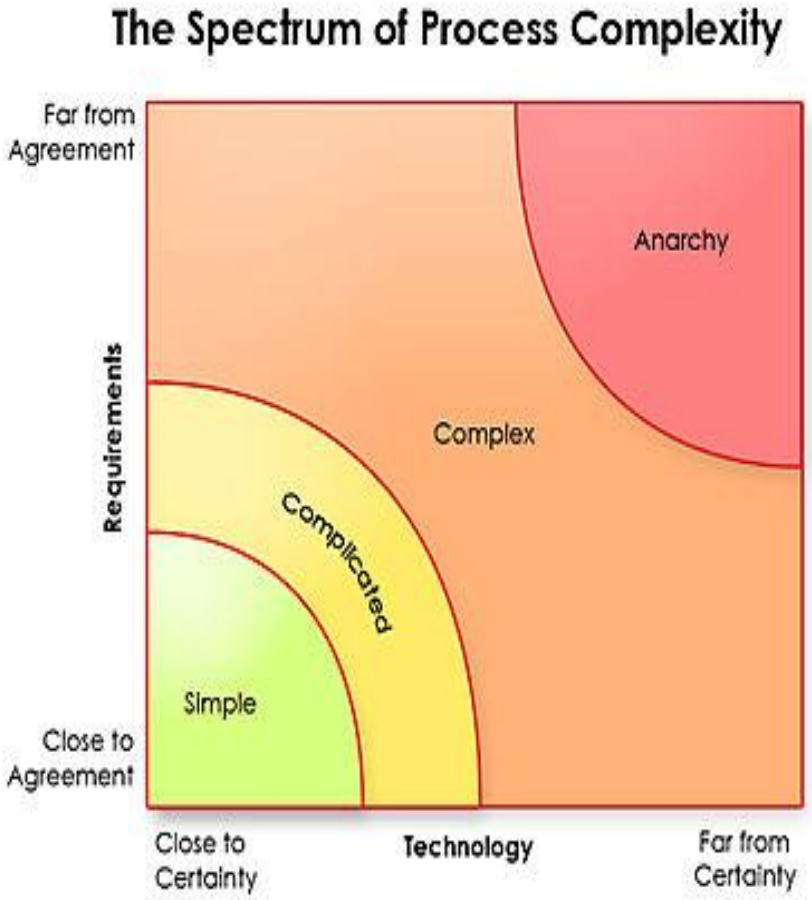
Metodología tradicional…

…restringir el cambio
…ser predictivos
…difícil medir progreso

Metodología Ágil…

…abrazar el cambio
…ser adaptativo
…fácil medir progreso
…iterativos

¿Cuando funciona bien y cuando no?



Metodologías Tradicionales

Metodologías Ágiles

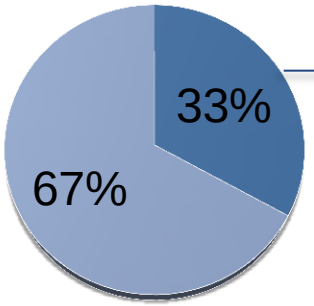
Manifiesto Ágil

- **Individuos e interacciones**
  sobre procesos y herramientas
- **Software funcionando**
  sobre documentación extensiva
- **Colaboración con el cliente**
  sobre negociación contractual
- **Respuesta ante el cambio**
  sobre seguir un plan

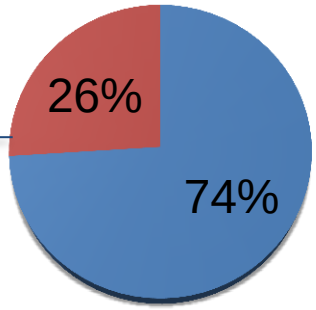
¿Porque el esfuerzo?

- ✓ Alta productividad y bajos costos
- ✓ Mejora del compromiso del trabajador
- ✓ Mejores tiempos de salida al mercado
- ✓ Alta calidad
- ✓ Mejora de la satisfacción del cliente

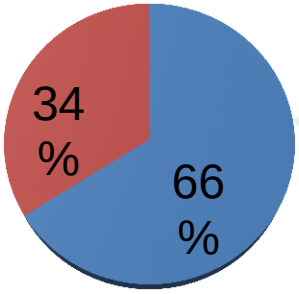
Beneficios de implementar Ágil



67% de las organizaciones encontraron que Ágil ha **mejorado** la **frecuencia de release** de sus productos *Mayo 2009 –Forrester Research*



74% de las organizaciones encontraron que las prácticas Ágiles han **aumentado** la **productividad** *2008 State of Agile - VersionOne*



66% de las organizaciones encontraron **reducción de costos** en mas de un 10%
2008 State of Agile - VersionOne

Problema de estudio

Pregunta de investigación

Como …

Cuales son los obstáculos que aparecen al construir seguridad en proyectos Ágiles

De organizaciones donde…

- ✓ **La seguridad no es un jugador principal**
- ✓ **Esquema de negocio de *software factory***
- ✓ **Recursos incorporados en demanda**
- ✓ **Equipos multidisciplinarios de diferentes *skills***
- ✓ **No se encuentra estructurada en áreas funcionales**

Propuestas de construcción de seguridad I

Implementación de un *Security Development Lifecycle*

Puntos débiles:

- Introducción de prácticas de seguridad según las fases tradicionales de un proyecto
- Requieren de algún tipo de estructura de unidades funcionales en la organización.
- Presuponen la existencia de algún tipo de proceso y nivel de madurez

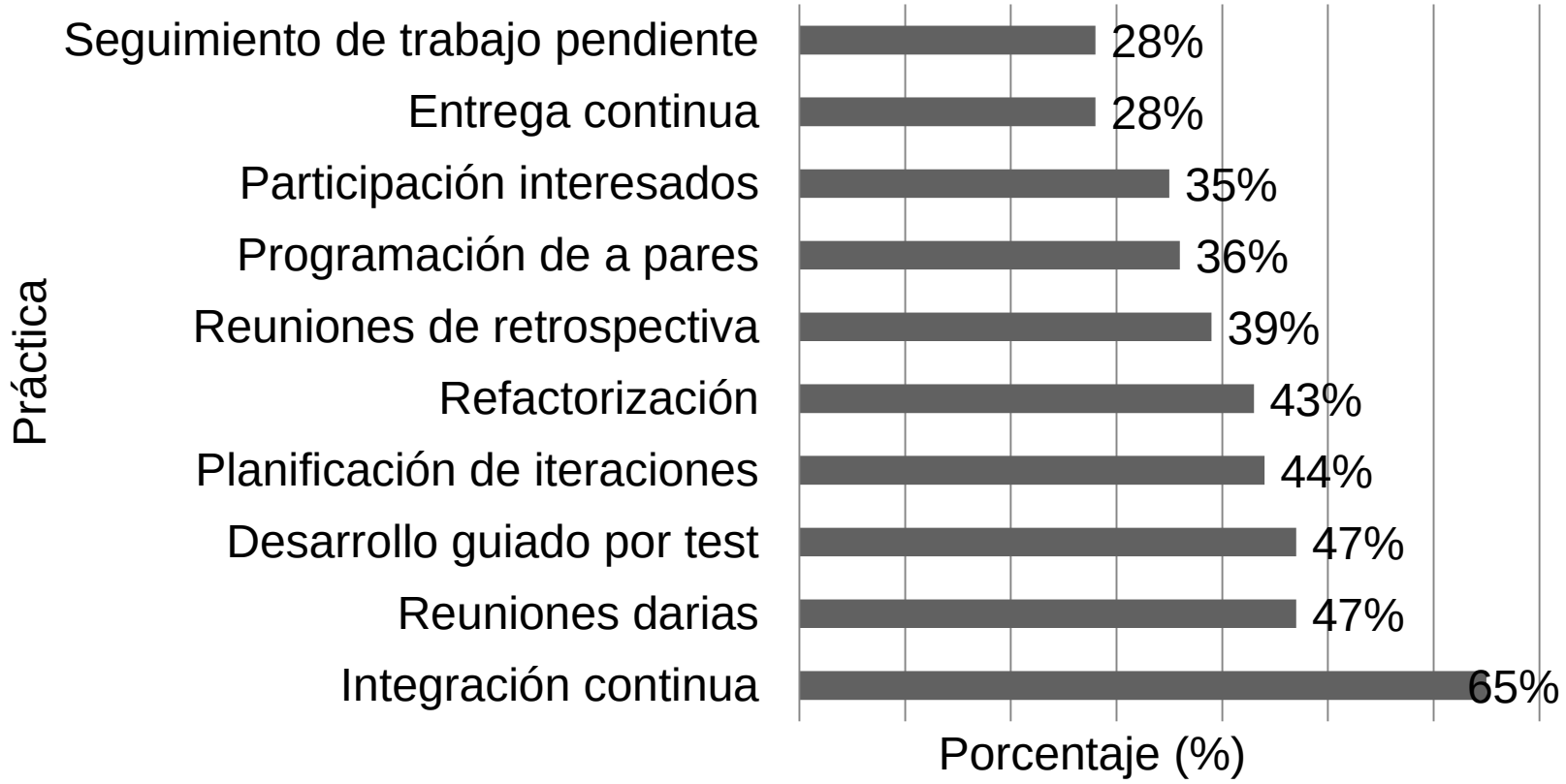
Propuestas de construcción de seguridad II

Utilizar prácticas Ágiles como punto de entrada para la construcción de seguridad

Puntos fuertes

- ✓ Eliminar malos hábitos presentes en el uso de prácticas Ágiles
- ✓ Dotar a la práctica Ágil un enfoque en seguridad para la construcción de funcionalidades seguras el cual no existe
- ✓ Funcionar como punto de transición para la adopción de iniciativas más complejas en el futuro

Prácticas Ágiles mas adoptadas



Objetivos del trabajo

1. Fomentar y motivar el uso de prácticas de seguridad en las metodologías Ágiles

2. Identificar razones que llevan al no uso de prácticas de seguridad en proyectos bajo estas metodologías

3. Crear una recomendación para la adopción de prácticas de seguridad aplicables a este tipo de proyectos

Experimentación

Contexto

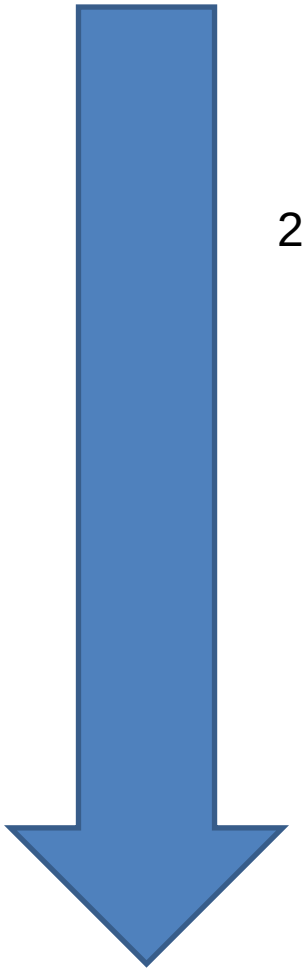
- Aplicaciones de comercio electrónico
- Gestión de información sensitiva
- Aplicación de metodologías Ágiles
- Equipo sin experiencia en seguridad
- Desarrollo sin implementación de practicas de seguridad

Procedimiento

1. Selección de una muestra

2. Observación del uso de prácticas Ágiles, visión y roles de seguridad en el campo de trabajo

3. Uso y propuesta de prácticas ágiles con foco en la seguridad

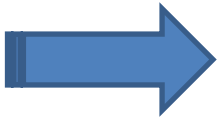


Análisis, conclusiones y nuevas hipótesis

Equipo Objeto de Estudio

1 SSR. DEV
1 SR. DEV

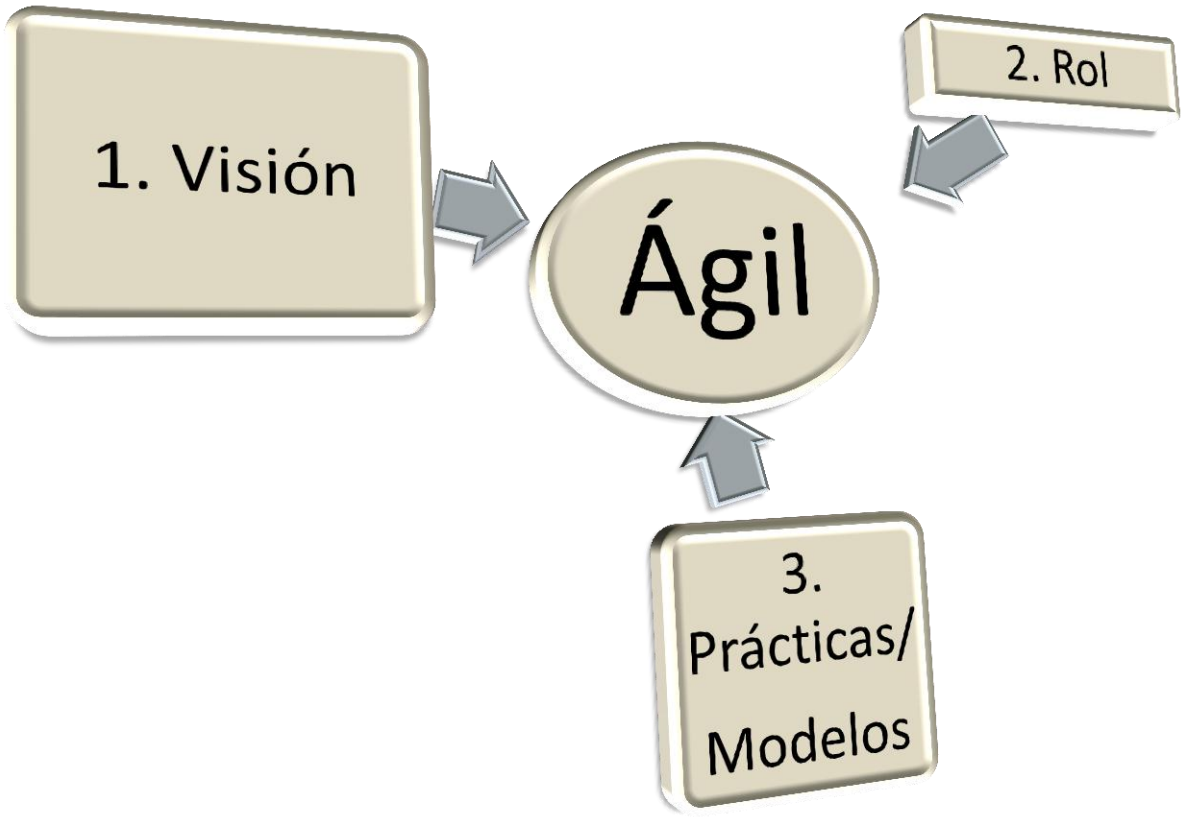
1 Líder técnico
1 Manager



1 SSR. Tester

Scrum

Clasificación de hallazgos



Vision de la seguridad

- Dependencia de factores internos y externos a la organización
- Valor de la información que maneja el sistema
- Correspondiente a etapas de post-liberación
- Dependiente del alcance y los costos
- Poca participación en entrenamientos

Rol de la seguridad

- Desconocimiento de este rol
- Hay dudas sobre como incorporar este rol
- No existen fondos destinados entrenamientos

Prácticas utilizadas

- No se han utilizado prácticas de seguridad
- Existen dificultad en la aplicación de la metodología Ágil
- Tiempos excesivamente no alcanzan

Propuesta de cambio sugerida al equipo

Comenzar a otorgar un enfoque en seguridad a las prácticas Ágiles utilizadas durante dos iteraciones

1. Planificación de iteraciones
2. Integración continua
3. Programación de a pares
4. *Whole team*

Resultado

Planificación de iteraciones se comenzó a incorporar historias de usuario relacionadas directamente con la seguridad de los requerimientos.

Integración continua el proceso no se utilizó solamente para verificar la correcta compilación e integración del código fuente, sino que se incluyeron analizadores de código estático para la detección de *bugs*.

Programación de a pares: dejo de ser utilizada como una práctica de iniciación de nuevos programadores, y comenzó a utilizarse para evaluar decisiones de diseño y realizar revisiones de código; atacando la posibilidad de fallas y *bugs*.

Whole team: Se sugirió el uso de esta práctica.

Conclusiones

Obstaculos

- Dificultades al momento de adoptar una metodología Ágil
- Ausencia de un *mindset* focalizado en seguridad por parte de la organización
- La falta de conocimientos y controles de seguridad necesarios por parte de los desarrolladores
- Visión de la seguridad como algo externo al desarrollo del software

Recomendaciones para la Construcción de Seguridad

- Evaluación de madurez
- Desarrollo de una mentalidad segura
- Aplicación de practicas Ágiles como transición hacia prácticas más seguras
- Transferencia del conocimiento al equipo

Preguntas