



OWASP
★ ★ ★ ★ ★ ★ ★ ★
Venezuela Chapter



Todos Somos parte de la seguridad en el Desarrollo de Software...

Acerca de mí

- Especialista en Seguridad de la Información
- IBM ACE/ACSE y Oracle SCSAS - SCSECA
- Pentester de Aplicaciones Web & Móvil
- Líder OWASP Capítulo Venezuela



Seguridad de la Información

- Ausencia de políticas de Seguridad en el Desarrollo de Software.
- Falta de estrategias y métricas que involucren a la dirección global y áreas involucradas en el programa de aseguramiento de software y métricas acerca de la postura de seguridad de la organización.



Gestión y planificación de Proyectos

- Los responsables de proyectos creen que la seguridad no aporta ningún valor.
- La seguridad no es concebida como un proceso.
- Las organizaciones suelen premiar tiempos de entregas, usabilidad y eventualmente performance... NO Seguridad.



Diseño y Desarrollo

- Inexistencia de un plan para incrementar el conocimiento de seguridad entre el personal de desarrollo de software a través de entrenamientos y orientación en temas de seguridad pertinentes a funciones del trabajo individual.
- Los usuarios finales en general, no suelen demandar software inseguro.
- Ausencia de Proceso de SDLC.
- Poco espacio en el tiempo para atender vulnerabilidades, pues siempre están desarrollando...



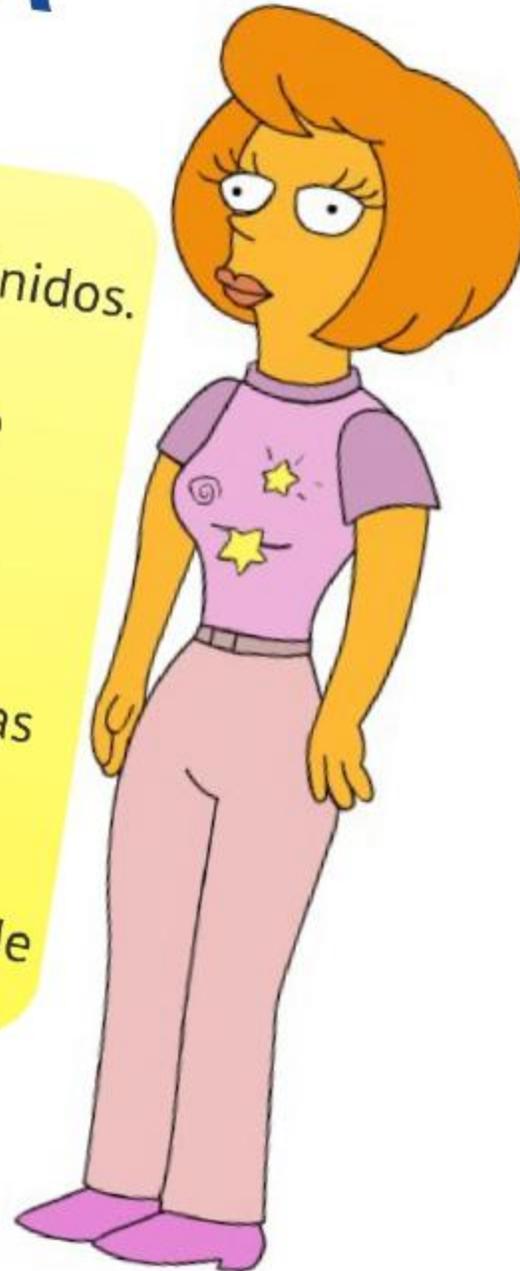
Desarrolladores

- Diseño orientado a funcionalidad.
- Desarrolladores sin entrenamiento en seguridad.
- Pobre conocimiento de amenazas.
- Ausencia de políticas de codificación segura.
- No emplean APIs de Seguridad.



DBA

- Privilegios de usuarios de aplicaciones no muy bien definidos.
- Ausencia de uso de técnicas de cifrado.
- Inexistencia de mecanismo de vistas para ocultamiento de tablas y columnas.
- Irregularidades al realizar copias de seguridad.



Sysadmin

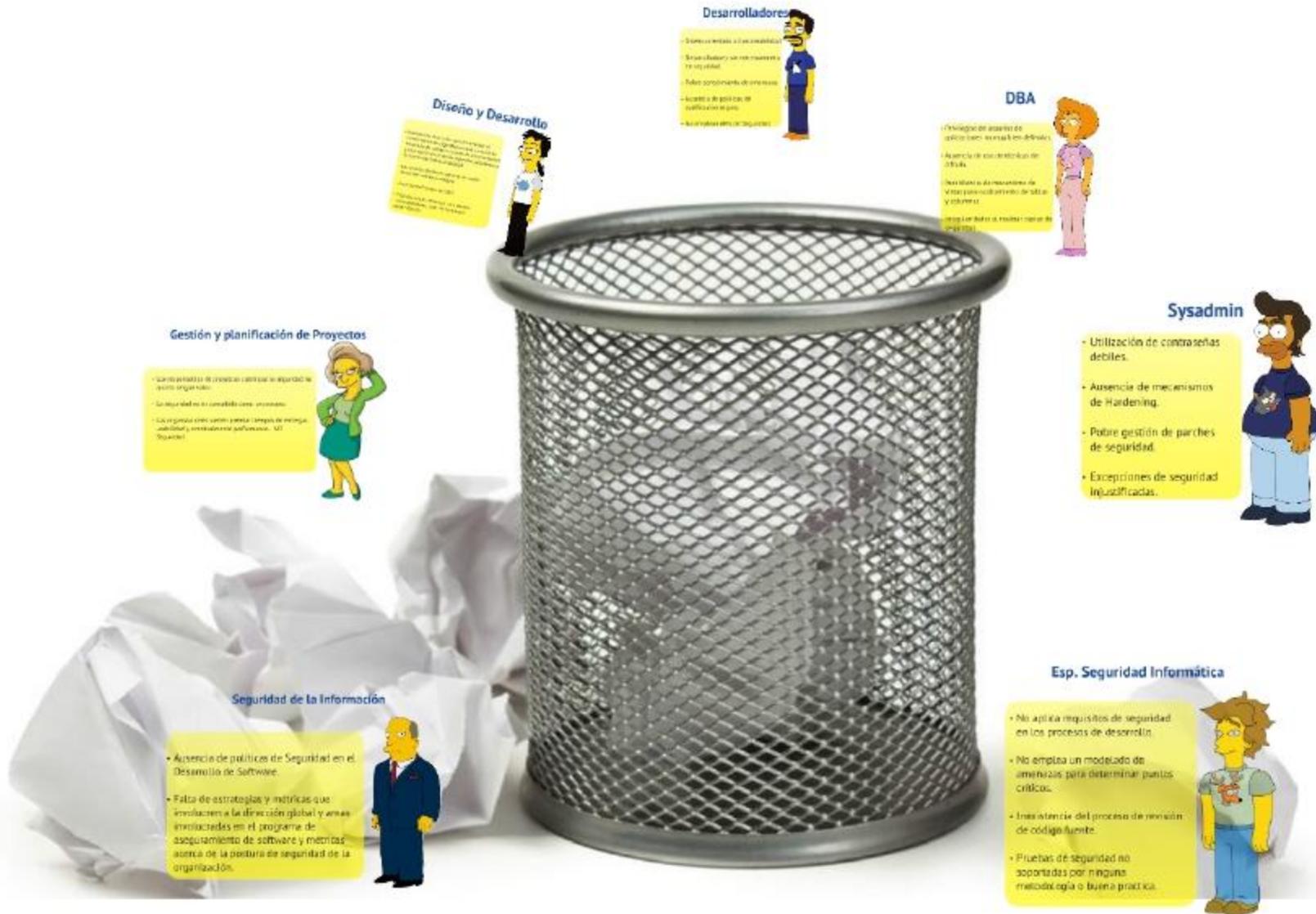
- Utilización de contraseñas debiles.
- Ausencia de mecanismos de Hardening.
- Pobre gestión de parches de seguridad.
- Excepciones de seguridad injustificadas.



Esp. Seguridad Informática

- No aplica requisitos de seguridad en los procesos de desarrollo.
- No emplea un modelado de amenazas para determinar puntos críticos.
- Inexistencia del proceso de revisión de código fuente.
- Pruebas de seguridad no soportadas por ninguna metodología o buena practica.





Todos Somos parte de la seguridad en el Desarrollo de Software...

P

E

O

Problemas

En la

Organización



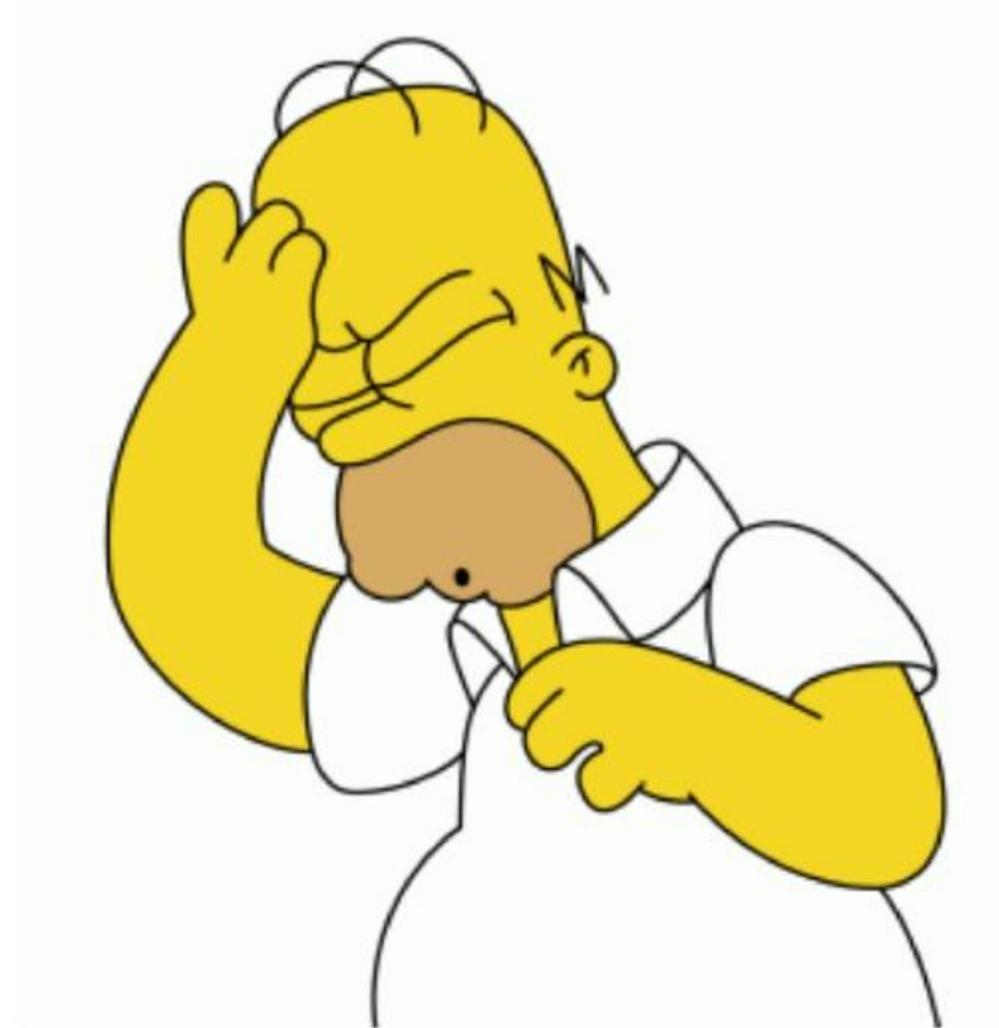
Y todos estos problemas no los llevamos a donde....



80% de las
Aplicaciones que
salen a
producción, **Son**
vulnerables.



XSS representa
el 53% entre las
vulnerabilidades
mas comunes
segun OWASP
TOP 10.



Coste de corrección de Vulnerabilidades



Diseño
(Cost = 1)



Implementación
(Cost = 6.5)

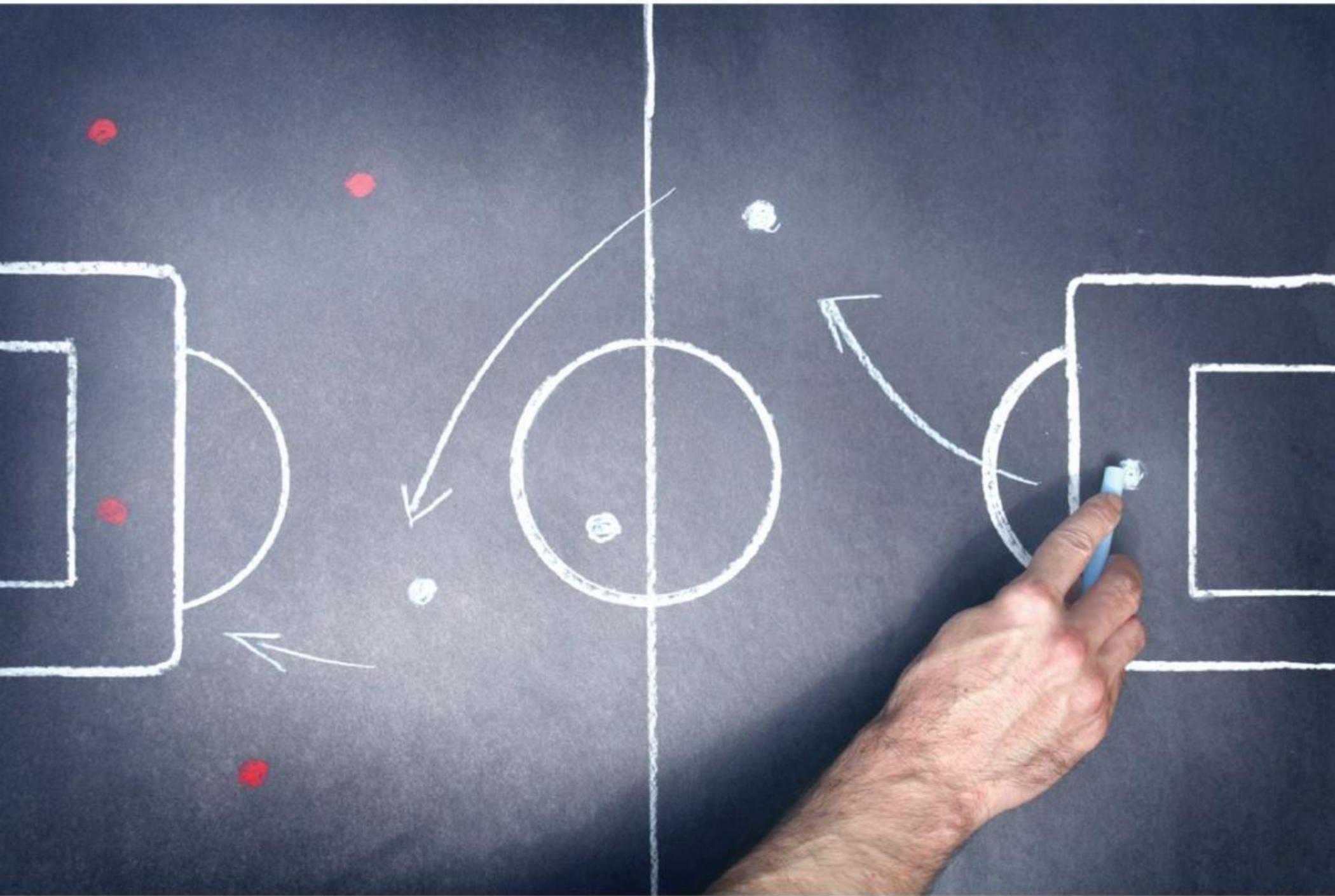


Testing
(Cost = 15)



Post Release
(Cost = 60)





Diseño y Desarrollo

- Definir y diseñar los requisitos de software.
- Desarrollar el código fuente del software.
- Realizar pruebas de integración y pruebas de aceptación.
- Mantener y actualizar el software.



Desarrolladores

- Crear software funcional y seguro.
- Trabajar en un entorno de desarrollo seguro y seguro.
- Seguir las mejores prácticas de desarrollo seguro.
- Trabajar con los equipos de Seguridad y Abusos de Seguridad.



DBA

- Definir un sistema para el desarrollo de pruebas y la gestión de subversiones.
- Utilizar técnicas para el desarrollo de pruebas.
- Utilizar mecanismos de defensa para el desarrollo de pruebas y la gestión de subversiones.
- Planificar la gestión de la configuración de datos de seguridad.



Gestión y planificación de Proyectos

- Analizar el impacto del proyecto en la vida del desarrollo de software.
- Definir el plan de implementación del software para el desarrollo de software.
- La seguridad debe ser un requisito de software, no un requisito de desarrollo de software.



Sysadmin

- Establecer segregación de ambientes (Desarrollo, Calidad y Producción).
- El Hardening debe ser obligatorio.
- Mecanismo de gestión de parches de seguridad.
- Excepciones de seguridad deben ser justificadas y llevadas a comité de riesgos tecnológicos.



Seguridad de la Información

- La dirección Seguridad de la Información debe establecer políticas de Seguridad en los procesos de Desarrollo de Software.
- Cumplimiento: Establecer una estructura de control y auditoría para asegurar el cumplimiento de regulaciones y alcanzar niveles óptimos en el aseguramiento de software bajo construcción y en operación.
- Involucrar a la dirección global y a las áreas de Desarrollo para establecer un modelo de madurez en la construcción del Software seguro.



Esp. Seguridad Informática

- Aplicar requisitos de seguridad en los procesos de desarrollo.
- Realizar modelados de amenazas según los criterios propios de cada aplicación.
- La revisión de código fuente debe ser un proceso constante, bien sea manual y/o automatizado.
- Las pruebas de seguridad deben llevarse de la mano bajo una metodología que permita calificar la evaluación, ejmp: Owaso Testing Guide.




Todos Somos parte de la seguridad en el Desarrollo de Software...

Seguridad de la Información

- La dirección Seguridad de la Información debera de establecer políticas de Seguridad en los procesos de Desarrollo de Software.
- Cumplimiento: Establecer una estructura de control y auditoria para asegurar el cumplimiento de regulaciones y alcanzar niveles óptimos en el aseguramiento de software bajo construcción y en operación.
- Involucrar a la dirección global y a las áreas de Desarrollo para establecer un modelo de madurez en la construcción del Software seguro.



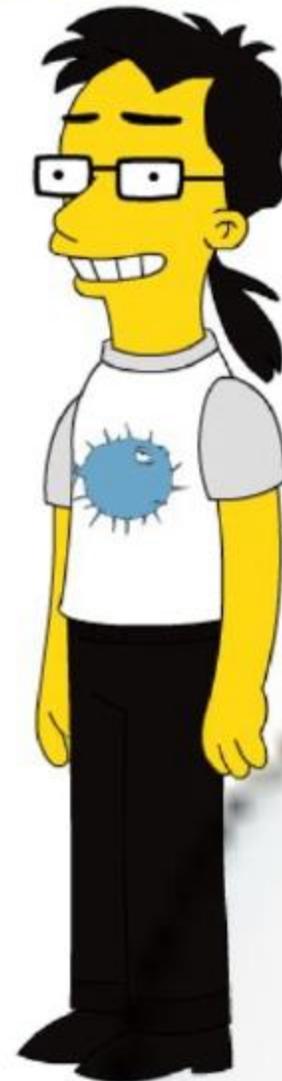
Gestión y planificación de Proyectos

- Establecer la seguridad como un proceso continuo en la vida del desarrollo de software.
- Establecer dentro de la planificación actividades que permitan el testeado de las mismas.
- La seguridad también debe ser premiada, gracias a ello se logran reducir en una gran cantidad el fraude o daño a la imagen de la organización.



Diseño y Desarrollo

- Solicitar a las áreas pertinente o empresas especializadas, la asesoría y adiestramiento en Desarrollo Seguro.
- Si hay Ausencia del Proceso de SDLC, tendran que crearlo e involucrar las actividades de seguridad en cada uno de los ciclos.
- Establecer un esquema de trabajo para mitigar las vulnerabilidades que se encuentren en la fase de testing y/o produccion segun sea el caso.
- Los Usuarios van a demandar Software Inseguro



Desarrolladores

- Diseño orientado a funcionalidad Y seguridad.
- Tendrán que ser intruidos en el uso de cotramedidas para remediar software inseguro.
- Su guia sera las políticas de codificación segura.
- Tendrán que usar APIs de Seguridad y bibliotecas de codigo seguro.



DBA

- Definir un esquema para el otorgamiento de privilegios a usuarios de aplicaciones
- Utilizar buenas practicas en las técnicas de cifrado.
- Establecer mecanismo de vistas para ocultamiento de tablas y columnas segun especificaciones de seguridad.
- Planificar la gestion para la realizacion de copias de seguridad.



Sysadmin

- Establecer segregación de ambientes (Desarrollo, Calidad y Producción).
- El Hardening debe ser obligatorio.
- Mecanismo de gestión de parches de seguridad.
- Excepciones de seguridad deben ser justificadas y llevadas a comite de riesgos tecnologicos



Esp. Seguridad Informática

- Aplicar requisitos de seguridad en los procesos de desarrollo.
- Realizar modelados de amenazas según los criterios propios de cada aplicación.
- La revisión de código fuente debe ser un proceso constante, bien sea manual y/o automatizado.
- Las pruebas de seguridad deben llevarse de la mano bajo una metodología que permita calificar la evaluación, ejmp: Owasp Testing Guide.



Diseño y Desarrollo

- Definir y validar los requisitos de software.
- Diseñar la arquitectura de software.
- Desarrollar el código fuente del software.
- Realizar pruebas de desarrollo.
- Integrar y validar el software.
- Mantener el software.



Desarrolladores

- Crear software funcional y seguro.
- Trabajar con un modelo de desarrollo seguro.
- Lograr los requisitos de seguridad.
- Trabajar con los estándares de seguridad y habilidades de seguridad.



DBA

- Definir un sistema para el desarrollo de programación y la gestión de subconsultas.
- Utilizar técnicas para el mantenimiento de datos.
- Utilizar mecanismos de backup para el mantenimiento y optimización de bases de datos.
- Planificar la gestión de los recursos de bases de datos.



Gestión y planificación de Proyectos

- Analizar la capacidad como un proceso continuo en la vida del desarrollo de software.
- Establecer planes de implementación de software con planes de riesgo de un proyecto.
- La seguridad debe ser un requisito de diseño y de desarrollo.



Sysadmin

- Establecer segregación de ambientes (Desarrollo, Calidad y Producción).
- El Hardening debe ser obligatorio.
- Mecanismo de gestión de parches de seguridad.
- Excepciones de seguridad deben ser justificadas y llevadas a comité de riesgos tecnológicos.



Seguridad de la Información

- La dirección Seguridad de la Información debe establecer políticas de Seguridad en los procesos de Desarrollo de Software.
- Cumplimiento: Establecer una estructura de control y auditoría para asegurar el cumplimiento de regulaciones y alcanzar niveles óptimos en el aseguramiento de software bajo construcción y en operación.
- Involucrar a la dirección global y a las áreas de Desarrollo para establecer un modelo de madurez en la construcción del Software seguro.



Esp. Seguridad Informática

- Aplicar requisitos de seguridad en los procesos de desarrollo.
- Realizar modelados de amenazas según los criterios propios de cada aplicación.
- La revisión de código fuente debe ser un proceso constante, bien sea manual y/o automatizado.
- Las pruebas de seguridad deben llevarse de la mano bajo una metodología que permita calificar la evaluación, ejmp: Owaso Testing Guide.




Todos Somos parte de la seguridad en el Desarrollo de Software...



YouTube

Preguntas?





@3ddavid

<http://www.3ddavid.net>

ed david01@gmail.com

edgar.salazar@owasp.org