VIII Jornada Nacional de Seguridad Informática

ACIS

Gestión de la inseguridad de las aplicaciones: Un enfoque práctico

Desca
The Networking Company

FELIPE ANTONIO SILGADO QUIJANO
CISSP®, CISM®, ISO 27001 LEAD AUDITOR,
ABCP, ITIL® FOUNDATION CERTIFICATE

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP

CISM
CERTIFIED INFORMATION SECURITY MANAGER

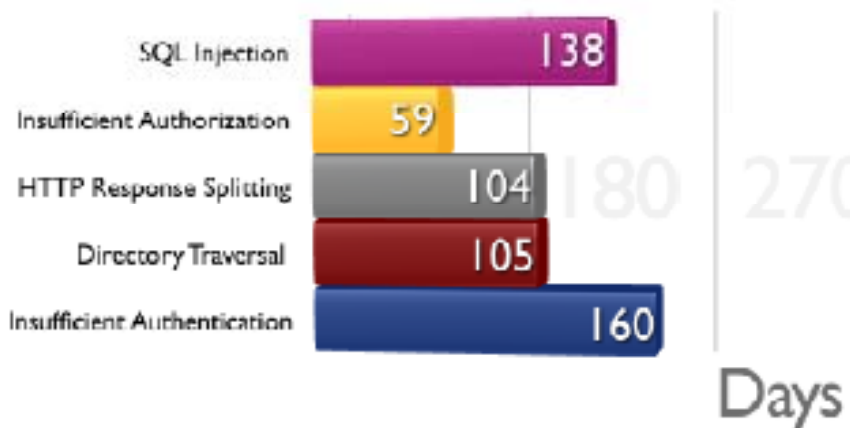
Agenda

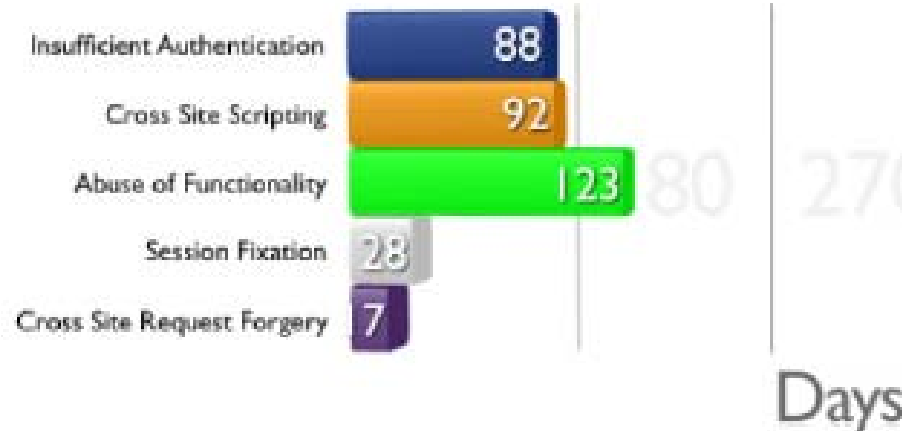
- Algunas estadísticas
- Problemática actual
- Gestionando la Inseguridad en las aplicaciones
- Conclusiones
- Información adicional
- Preguntas

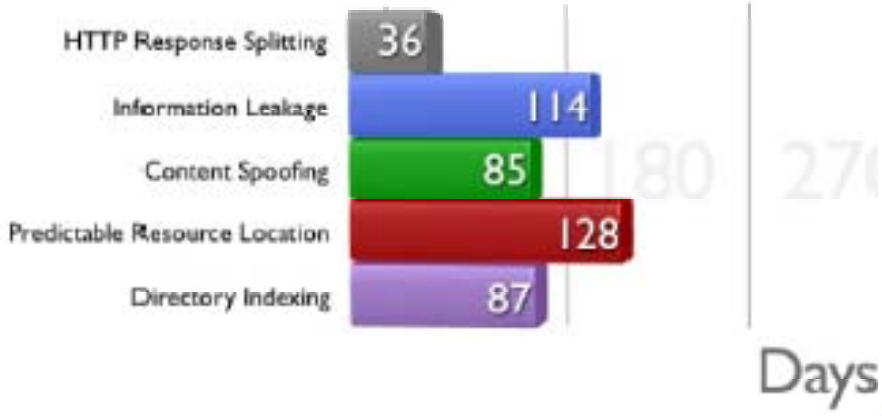
Algunas estadísticas

Reporte de Q1 de 2008. White Hat Security	• 9 de 10 sitios web tienen, al menos, una vulnerabilidad significativa. • En promedio cada sitio Web tiene 7 vulnerabilidades. • En promedio uno de cada seis sitios Web es vulnerable a inyección de código SQL
Global Security Survey 2007. Deloitte	• El 87% de los encuestados siente que la calidad en el desarrollo del software es pobre y que es una de las amenazas top que viene en los próximos 12 meses.
VII Encuesta Nacional de Seguridad Informática. ACIS	• 40% de las compañías invierten presupuesto de seguridad en desarrollo y afinamiento de seguridad de las aplicaciones.

Algunas estadísticas

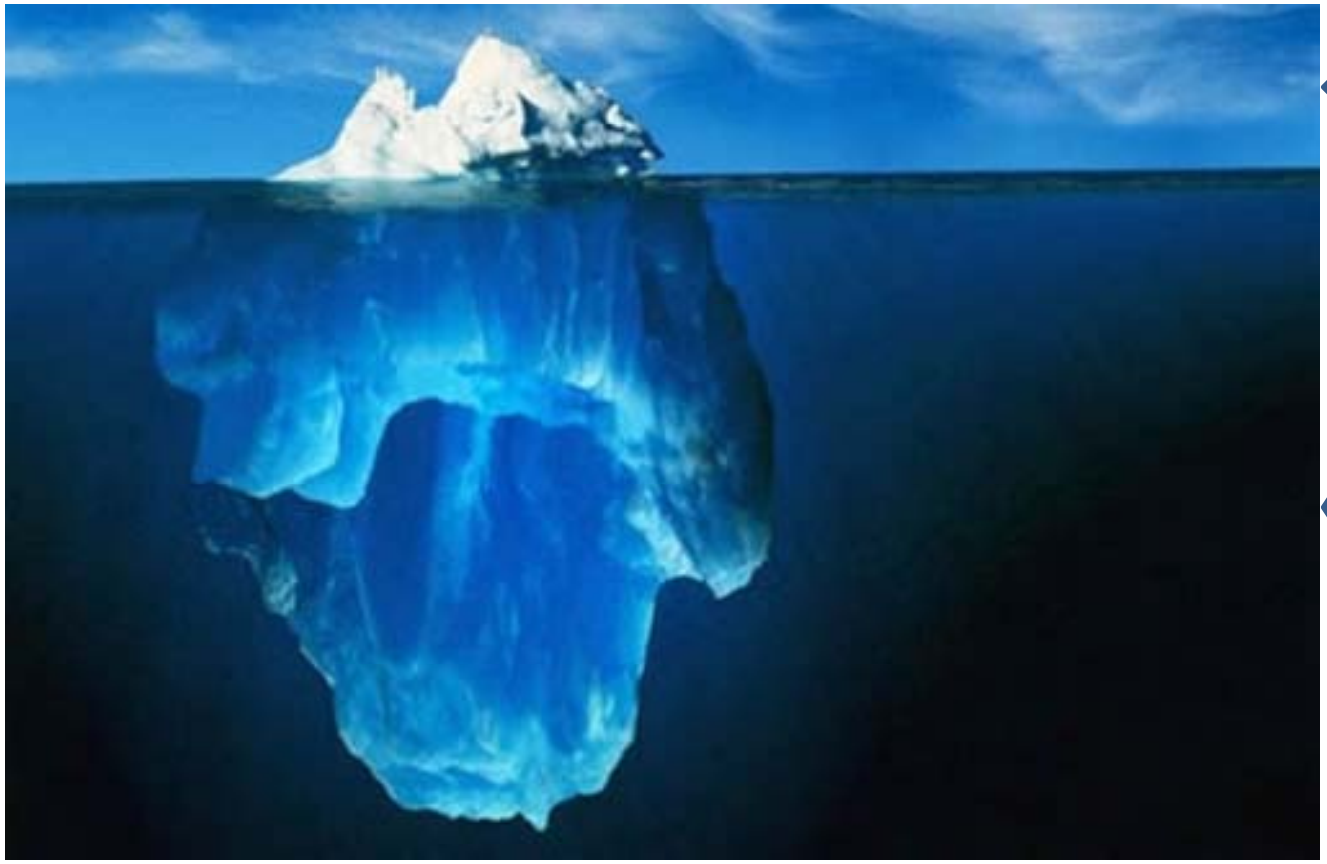






White Hat Security Report Q1 2008

Problemática actual



Los requerimientos que hoy se tienen en cuenta

Los requerimientos que hace falta tener en cuenta

Problemática actual

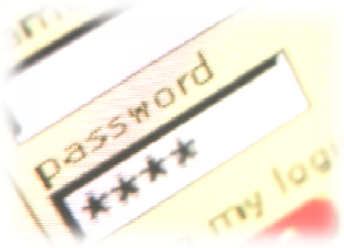
- No hay alineación estratégica
  - La planeación estratégica del negocio no está alineada a la planeación estratégica de seguridad. Se hace planeación estratégica de seguridad?
  - Los objetivos de la compañía no son conocidos por el área de seguridad
  - Los requerimientos de seguridad no hacen parte de los requerimientos de las aplicaciones.

Problemática actual

- No hay entrega de valor al negocio
  - Las áreas de negocio no tienen visibilidad del valor que puede entregar el área de seguridad.
- No hay gobierno de seguridad
  - No existe generalmente una política que indique la posición de la empresa frente a la seguridad de las aplicaciones, mucho menos un proceso de Gestión de Seguridad de Aplicaciones o un Sistema de Gestión de Seguridad de la Información (SGSI).

A qué se refiere: seguridad en aplicaciones?

- Según al Global Security Survey 2007 de Deloitte, la seguridad en las aplicaciones se refiere a:
  - *"… significa que hay un código seguro, integrado en la etapa de desarrollo, para prevenir vulnerabilidades potenciales y que los pasos tales como pruebas de vulnerabilidad, escaneo de aplicaciones y pruebas de penetración son parte del ciclo de vida de desarrollo de software de una organización."*



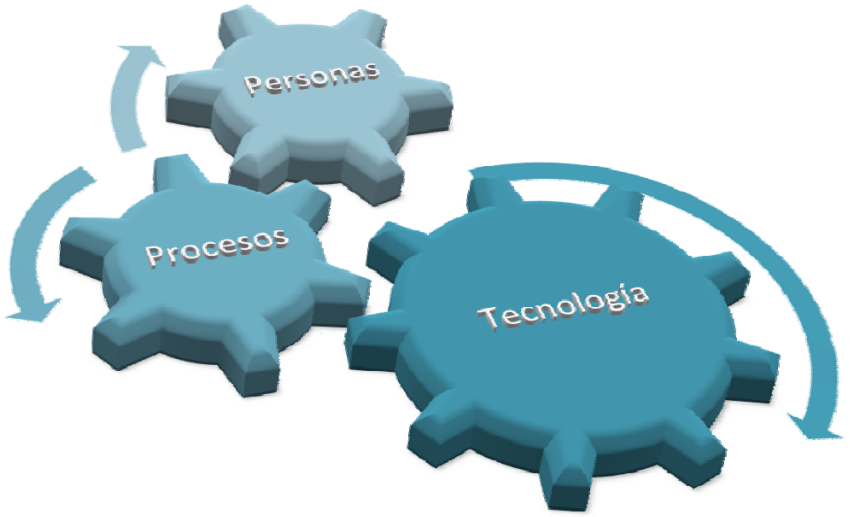
A qué se refiere: seguridad en aplicaciones?

- La seguridad en las aplicaciones va mas allá de controlar el acceso utilizando un usuario y password, o de colocar el servidor web en una dmz.
- Va mas allá de simplemente ejecutar un Hacking Etico 2 o 3 veces al año y reparar las vulnerabilidades para cerrar las brechas de riesgo.
- Va mas allá de reaccionar cada vez que hay una intrusión para desarrollarle un “parche” a la aplicación.

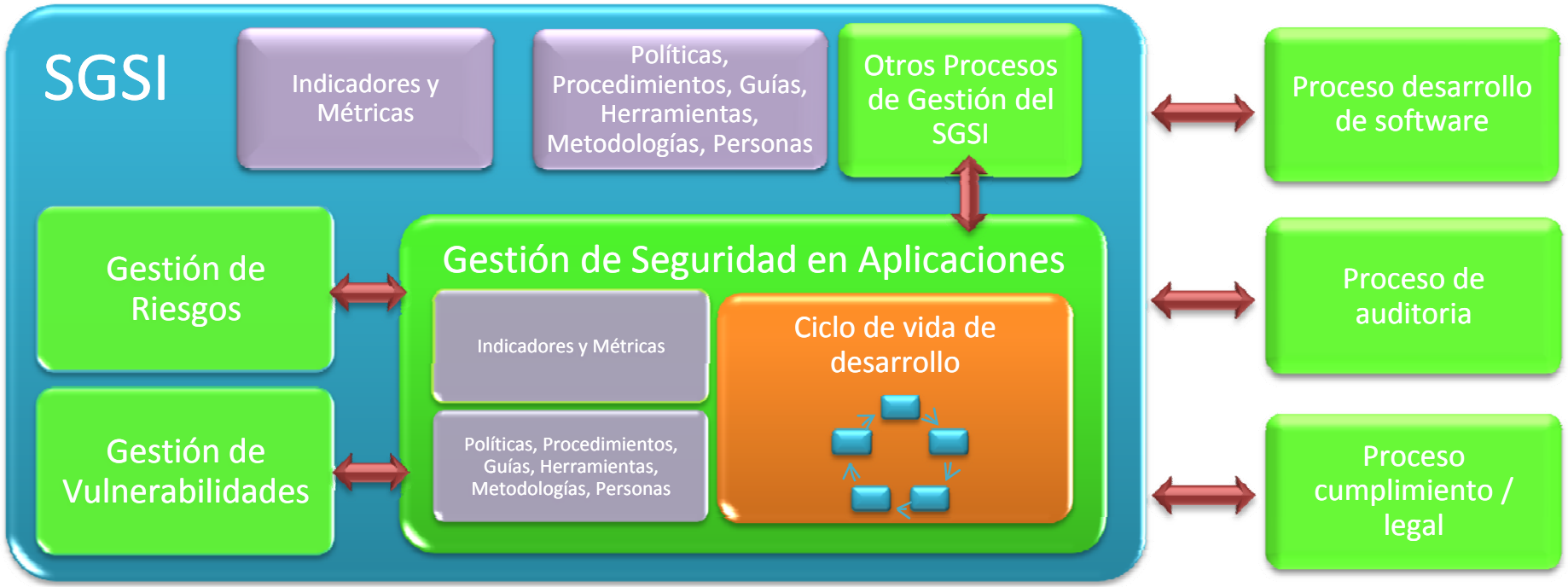
La seguridad de aplicaciones debe convertirse en un proceso de gestión!

Gestionando la inseguridad en las aplicaciones

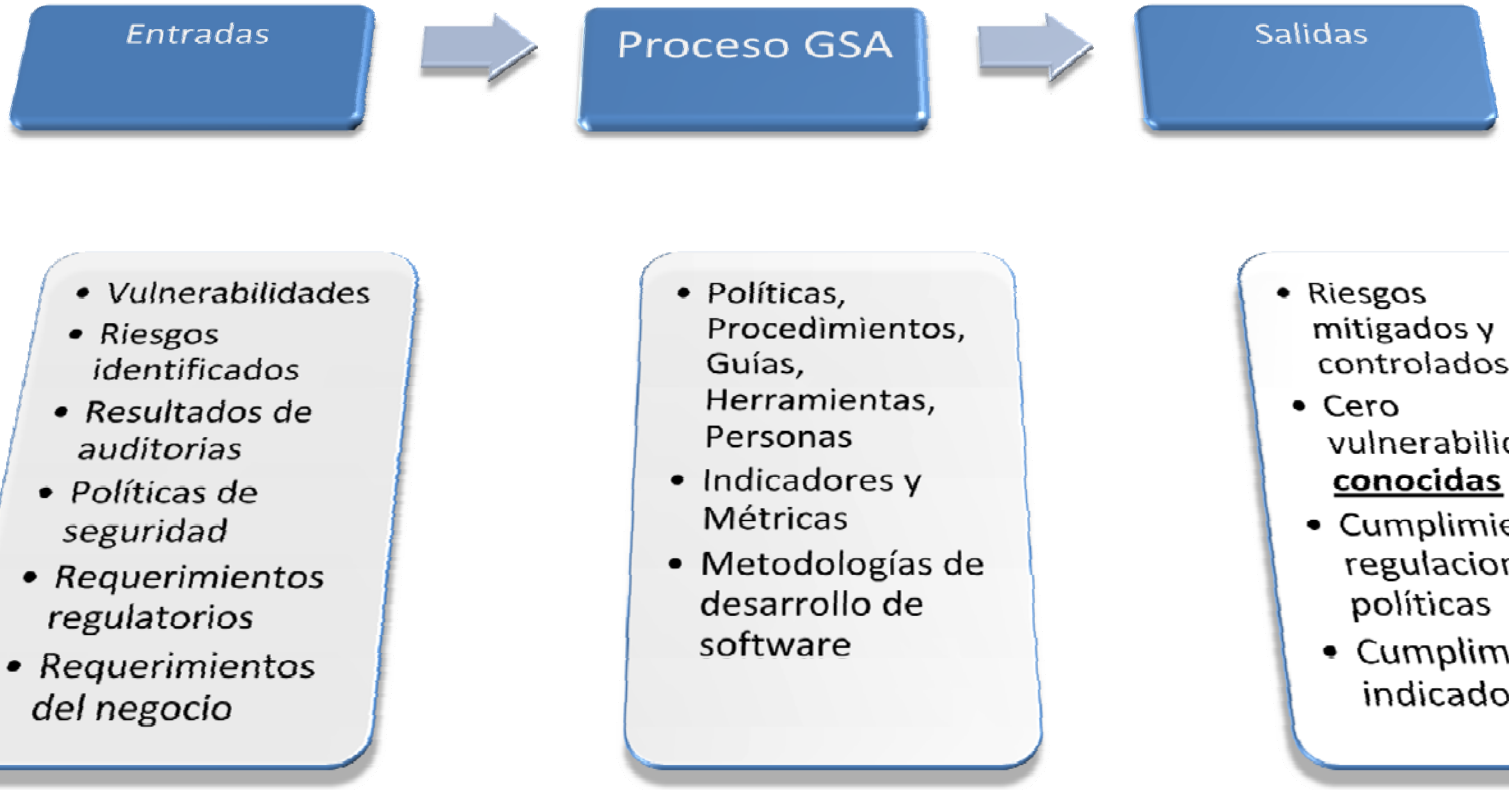
- Proceso de gestión
- Ciclo Continuo → Enfoque preventivo
- Componentes del proceso:
  - ✓ Entradas y Salidas
  - ✓ Objetivos / Metas
  - ✓ Políticas
  - ✓ Procedimientos
  - ✓ Responsables
  - ✓ Metodologías
  - ✓ Herramientas
  - ✓ Indicadores y métricas



Gestionando la inseguridad en las aplicaciones



Proceso de Gestión de Seguridad de Aplicaciones



Proceso de Gestión de Seguridad de Aplicaciones

- Objetivos /Meta
  - Garantizar que la seguridad es parte integral de los sistemas de información (ISO/IEC 17799:2005, pág. 77).
  - Asegurar que los requerimientos de seguridad necesarios son identificados, diseñados, implementados y probados, acorde al resultado del análisis de riesgos del sistema de información.
  - Asegurar que las aplicaciones tienen suficientes controles de seguridad que garanticen la protección de la información contenida en estas, de manera eficaz y eficiente.

Proceso de Gestión de Seguridad de Aplicaciones

- Políticas
  - Toda aplicación debe llevar a cabo un proceso de autenticación que asegure la identificación de manera única de los usuarios que acceden la información contenida en la aplicación.
  - Toda aplicación debe permitir controlar el acceso a la información mediante roles, perfiles o funciones por usuario.
  - Toda la información confidencial utilizada dentro de la aplicación debe permanecer cifrada durante su almacenamiento y transporte.
  - Toda aplicación debe llevar un registro de auditoria, que contenga todas las acciones realizadas por los usuarios.

Proceso de Gestión de Seguridad de Aplicaciones

- Procedimientos
  - Especificación y análisis de requerimientos de seguridad
  - Definición/Modificación de la arquitectura de seguridad
  - Revisión de cambios en la seguridad de las aplicaciones
  - Pruebas de controles de seguridad

Proceso de Gestión de Seguridad de Aplicaciones

- Personas / Responsables
  - Oficial de Seguridad de la Información
    - Velar porque las políticas de seguridad en aplicaciones se cumplan.
    - Velar porque el proceso de gestión GSA se ejecute.
    - Velar por el mejoramiento continuo de la seguridad en las aplicaciones.
    - Velar porque las aplicaciones en producción estén libres de problemas de seguridad.
  - Gerente de IT / Desarrollo de Software
    - Asegurar que los controles de seguridad de las aplicaciones son implementados.
    - Asegurar que en cada fase del ciclo de desarrollo de software se ejecutan las actividades relacionadas con seguridad.
  - Gerentes del negocio
    - Involucrar al área de seguridad en todos los negocios de la compañía

Proceso de Gestión de Seguridad de Aplicaciones

- Indicadores y métricas
  - Porcentaje de aplicaciones que pasaron por el proceso GSA
    - Meta: 100% de aplicaciones core de negocio
  - Porcentaje de aplicaciones probadas antes de salir a producción
    - Meta: 100% fueron probadas
  - Porcentaje de aplicaciones con riesgos de seguridad no mitigados
    - Meta: Menos del 10%
  - Porcentaje de aplicaciones que cumplen con las políticas de seguridad de aplicaciones
    - Meta: Mas del 90%

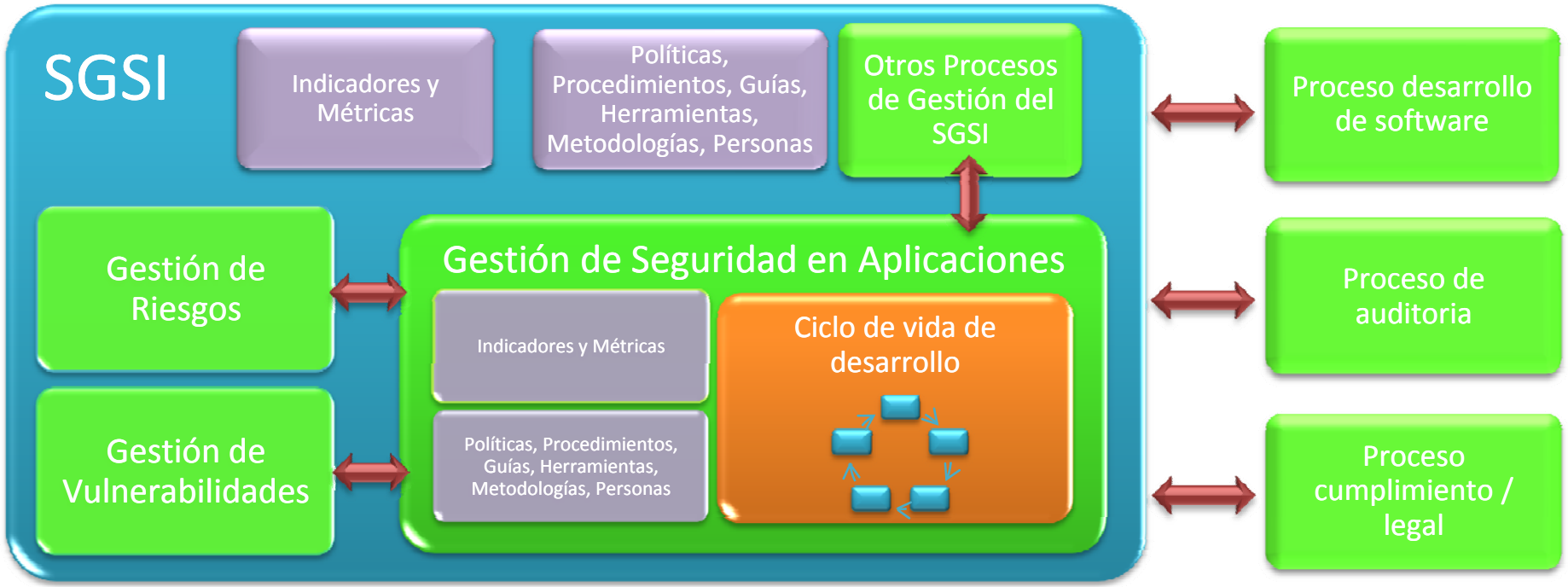
Proceso de Gestión de Seguridad de Aplicaciones

- Metodología de desarrollo de software
  - Dentro de cada fase de la metodología de desarrollo que se utilice, se deben incluir actividades propias de seguridad.
  - Cada fase del ciclo de desarrollo debe asegurar el cumplimiento de las políticas y estándares establecidos de seguridad.

Ciclo de Vida de Desarrollo de Software – Metodología de desarrollo en Cascada

Ciclo de Vida de Desarrollo de Software – Actividades de seguridad

Proceso de Gestión de Seguridad de Aplicaciones



Estándar para seguridad en aplicaciones

- La ISO está desarrollando la norma ISO/IEC 27034 Information technology -- Security techniques -- Guidelines for application security
- Esta norma tendrá una guía para el diseño y programación de aplicaciones. Dará guías sobre los controles de seguridad de la información relacionados con el ciclo de vida del desarrollo de sistemas de una compañía.
- La norma ISO/IEC 27034 Part 1, actualmente se encuentra en el primer borrador.

Fuente: http://www.iso27001security.com/html/27034.html

ISO

Conclusiones

- Las empresas tendrán que evolucionar de un enfoque de inseguridad de aplicaciones a un enfoque de gestión de seguridad de aplicaciones.
- Una gestión adecuada de seguridad de aplicaciones permitirá reducir los riesgos asociados a la confidencialidad, integridad y disponibilidad desde antes que la aplicación exista → enfoque preventivo

Información adicional

- www.owasp.org
- www.webappsec.org
- en.wikipedia.org/wiki/Web_application_framework
- whitepapers.zdnet.com/whitepaper.aspx?&scname=Application+Development&docid=345450
- www.computerworld.com/securitytopics/security/story/0,10801,106805,00.html
- www.utexas.edu/its/policies/opsmanual/appstd.php
- www.zone-h.org
- www.whitehatsec.com/home/resource/resource.html
- www.desca.com

Gracias

Felipe Silgado

CISSP®, CISM®, ISO 27001 Lead Auditor,

ABCP, ITIL® Foundation Certificate

fsilgado@desca.com

DESCA COLOMBIA

www.desca.com

“ Trust Desca, your BEST Information Security Partner ”