MODELOS DE DESARROLLO SEGURO DE SOFTWARE

Andrés Caro

Cátedra VIEWNEXT AN IBM SUBSIDIARY UEX

$whoami

Andrés Caro

- Profesor Titular de Universidad – Universidad de Extremadura
- Área Lenguajes y Sistemas Informáticos
- Doctor e Ingeniero en Informática
- Director Cátedra ViewNext-UEx Seguridad y Auditoría de Sistemas Software

- Grados de Ingeniería en Informática
  - Ingeniería de Computadores
  - Ingeniería del Software
- Máster en Ingeniería Informática

- Organización de cursos / jornadas
  - I Foro CIBER (noviembre 2016)
  - Curso Experto Profesional Derecho Tecnológico e Informática Forense
  - Hacking ético – Seguridad informática
  - LOPD – ENS
  - Peritaje – Informática forense

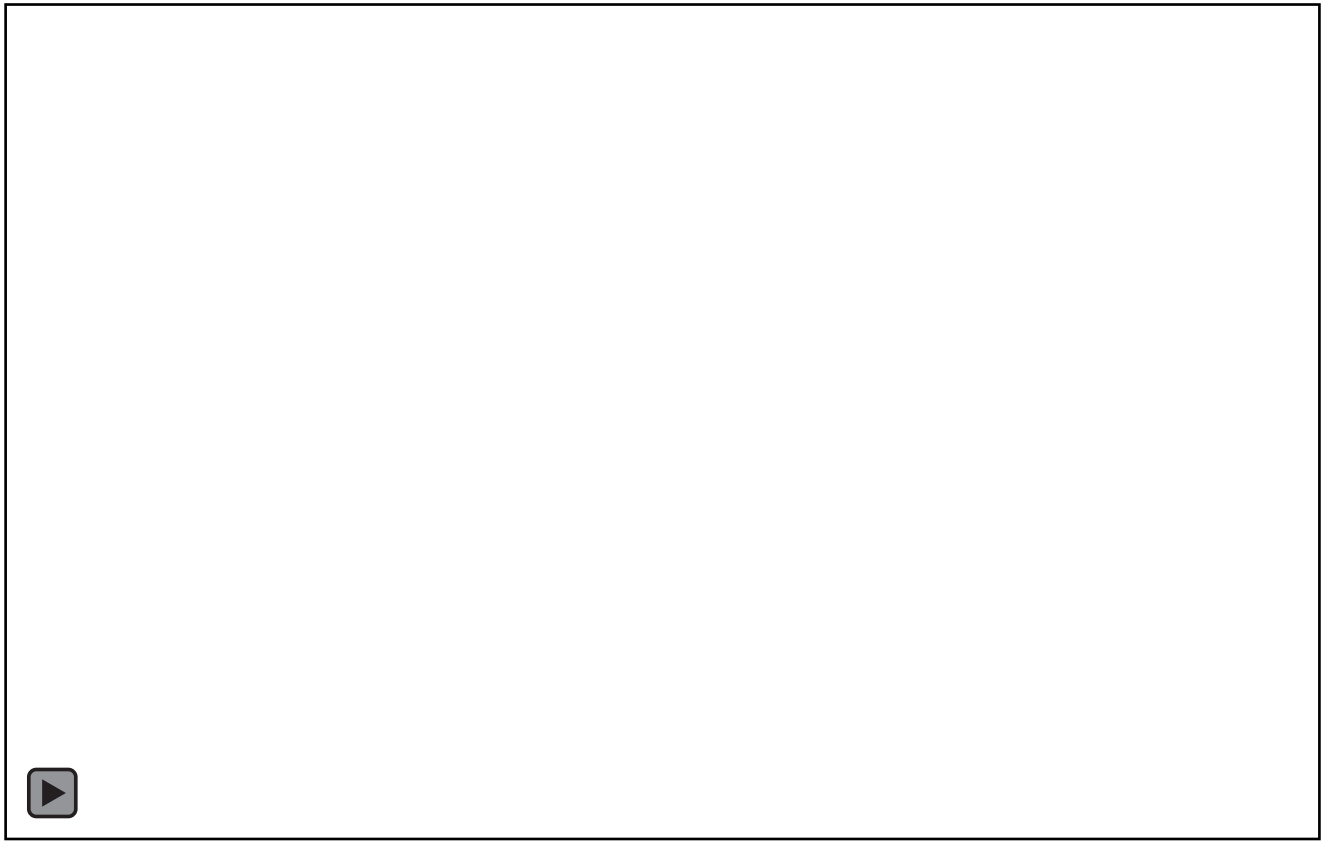
- Cibercooperante

@_AndresCaro_
andresc@unex.es

Por qué un modelo de desarrollo seguro (S-SDLC)

Necesidad: Ataques cibernéticos y coste de solucionar fallos

Multitud de ataques cibernéticos con graves consecuencias

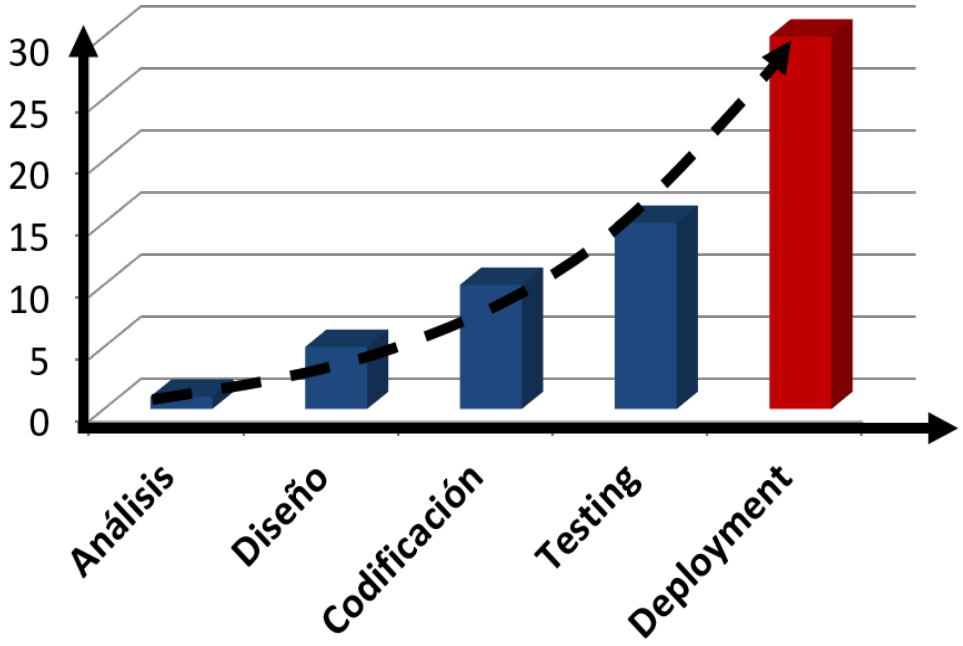


Fuente: http://map.norsecorp.com

Por qué un modelo de desarrollo seguro (S-SDLC)

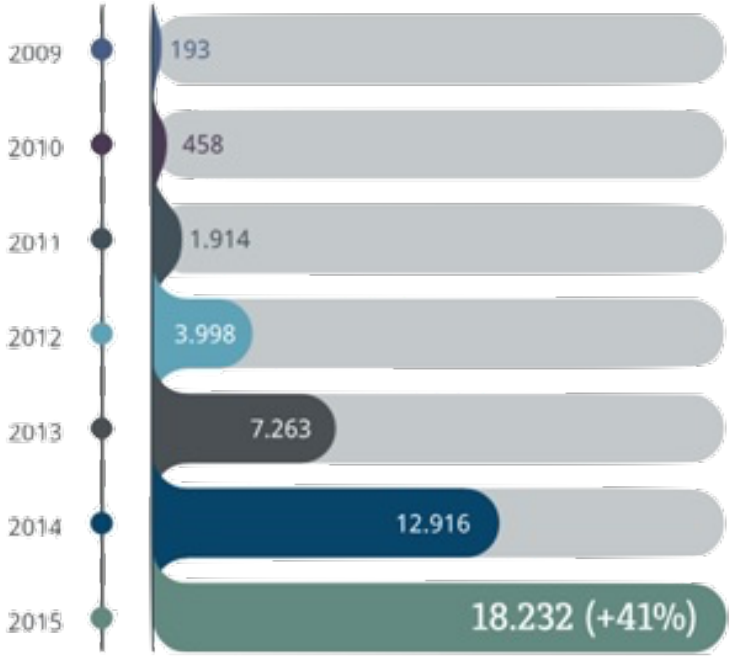
Necesidad: Ataques cibernéticos y coste de solucionar fallos

Coste de solucionar vulnerabilidades



Fuente: Instituto Nacional de Estándares y Tecnología (NIST)

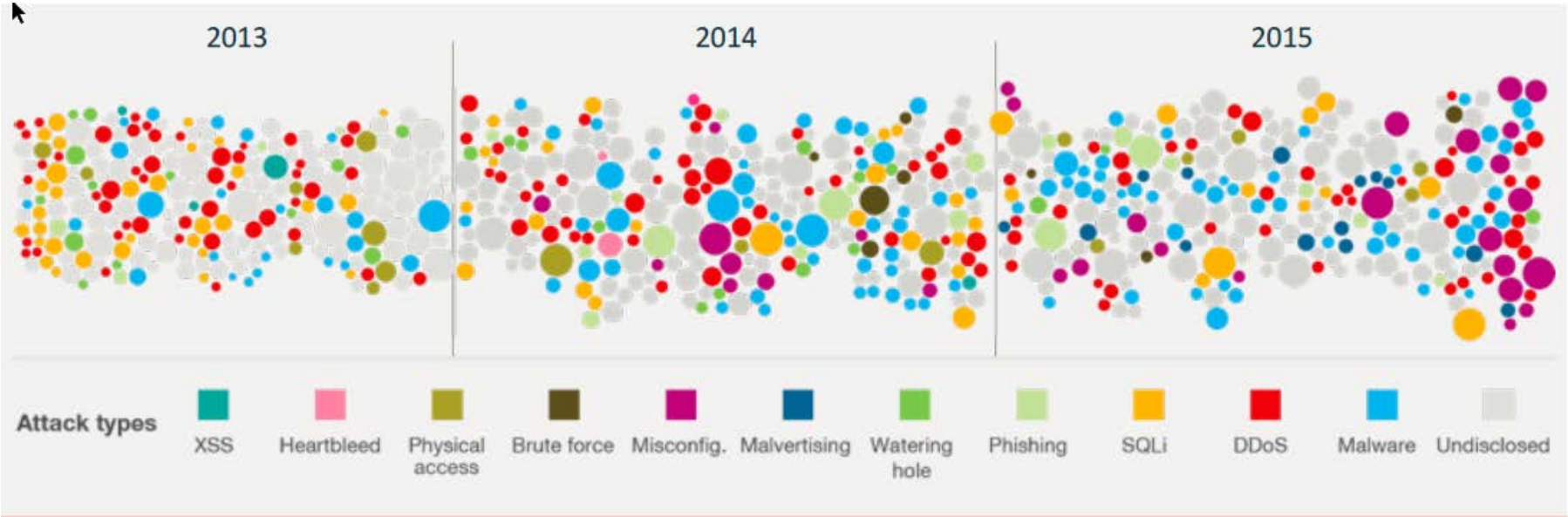
Incremento del +40% de los ciberataques en España



Fuente: (CCN-CERT)

Por qué un modelo de desarrollo seguro (S-SDLC)

Necesidad: Ataques cibernéticos y coste de solucionar fallos



Fuente: IBM Security Summit 2016

60 % de los ciberataques se cometen desde dentro (datos mundiales)

Fuente: IBM Security Summit 2016

Por qué un modelo de desarrollo seguro (S-SDLC)

Causas: Falta de seguridad desde el inicio de los proyectos

Falta de integración de seguridad en los procesos de desarrollo

Aplicar la seguridad en fases finales y más complejas de los proyectos

$=?

Consecuencias: altos costes, retrasos y reputación empresarial

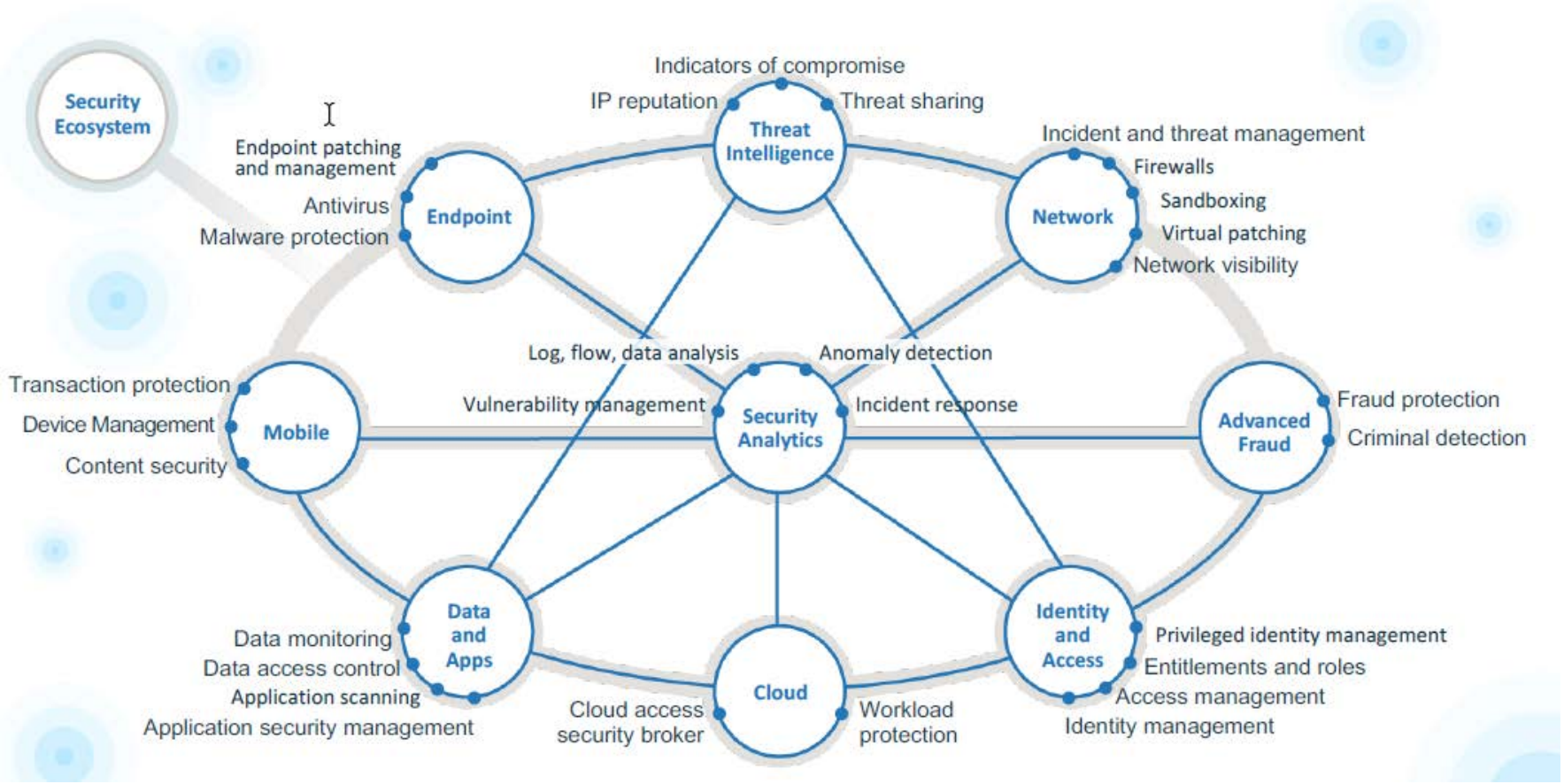
Pérdidas económicas

Pérdidas temporales

Pérdida de clientes
Confianza - Credibilidad

Por qué un modelo de desarrollo seguro (S-SDLC)

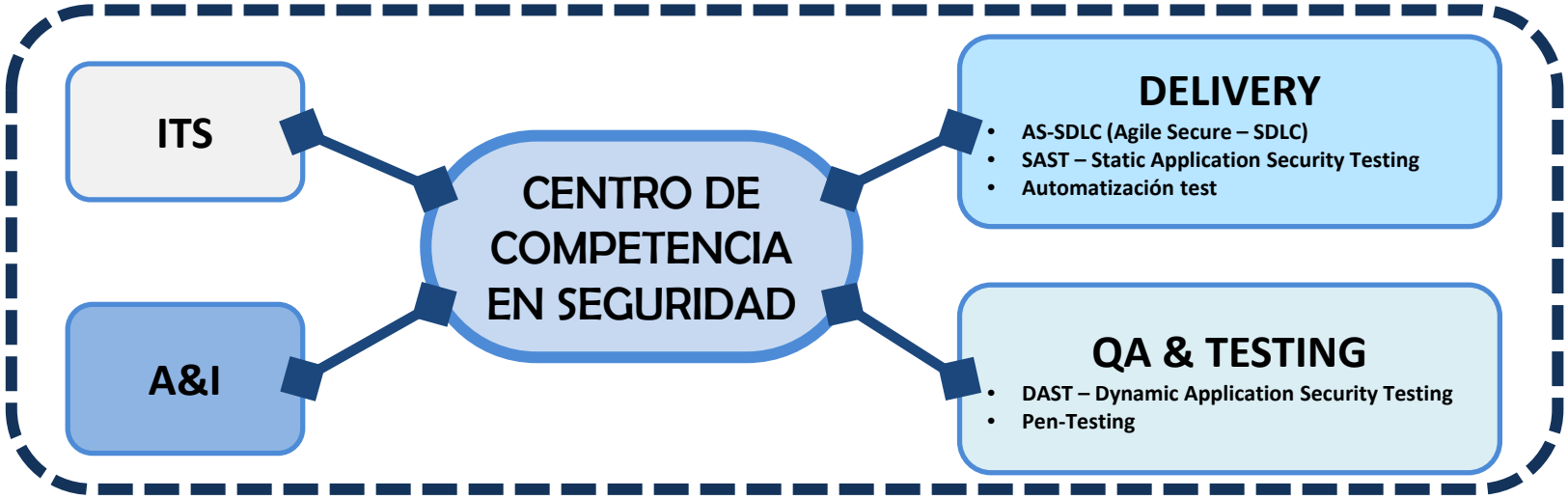
Necesidad: Generar una conciencia y cultura de la seguridad en las áreas implicadas en el ciclo de vida de un sistema



Fuente: IBM Security Summit 2016

Por qué un modelo de desarrollo seguro (S-SDLC)

Necesidad: Generar una conciencia y cultura de la seguridad en las áreas implicadas en el ciclo de vida de un sistema



Por qué un modelo de desarrollo seguro (S-SDLC)

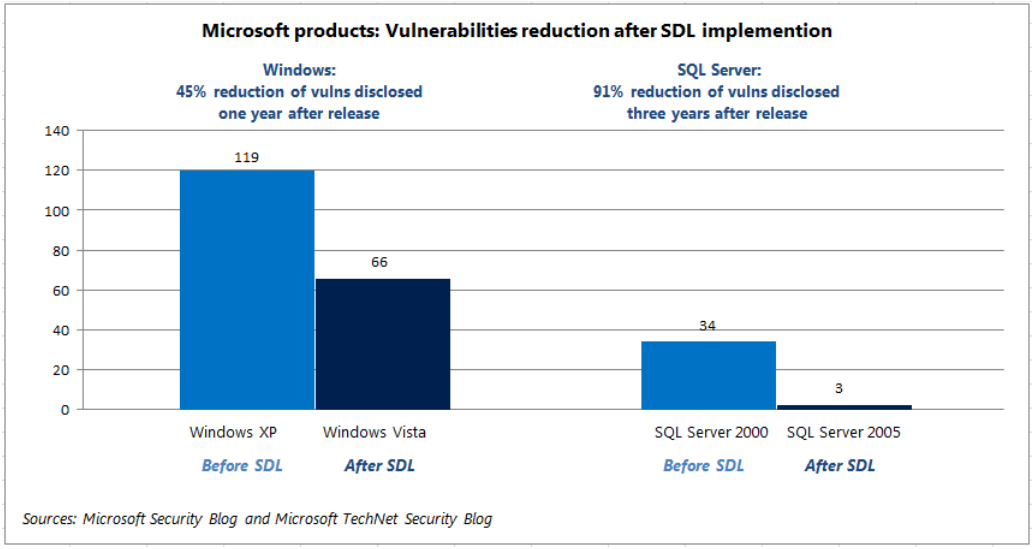
Análisis cuantitativo

75 % de las vulnerabilidades están relacionadas con las aplicaciones

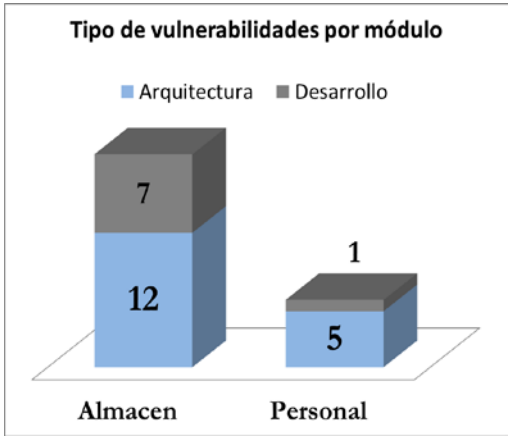
Reducción número de vulnerabilidades y criticidad:

- **Alrededor de un 40-50 % de reducción en el número de vulnerabilidades tras la implantación de un S-SDLC en el primer año (un 75-80 % sobre vulnerabilidades críticas).**

- Una reducción de un **50 %** en el número de vulnerabilidades implica una reducción de un **75%** en los costes de gestión de la configuración y respuesta a incidentes.



Fuente: Microsoft Security Blog & Microsoft Technet Security Blog



	Alto	Medio	Bajo	Informativo
PERSONAL	0	3	1	2
ALMACEN	1	9	4	5

40 % REDUCCIÓN*

* Haciendo una equiparación del tamaño de los módulos

Fuente: Piloto implantación proyecto EOSA

Por qué un modelo de desarrollo seguro (S-SDLC)

Análisis cuantitativo

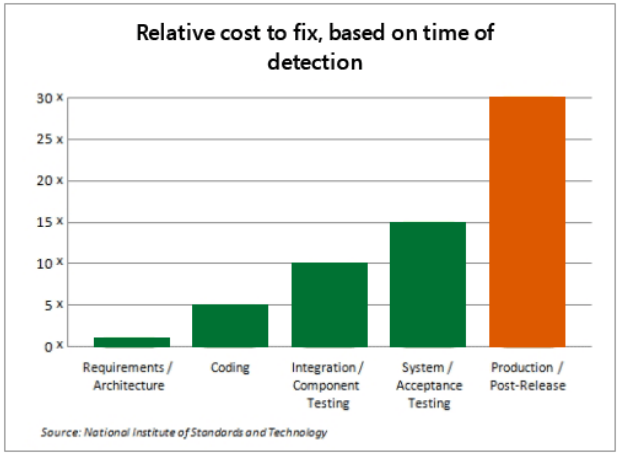
75 % de las vulnerabilidades están relacionadas con las aplicaciones

Reducción de costes de resolución de defectos:

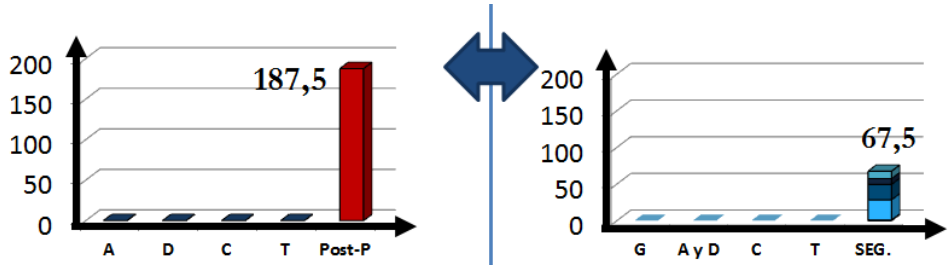
- **Alrededor de un 30 % de reducción en el coste de solucionar defectos y vulnerabilidades en una fase temprana del ciclo de desarrollo frente a realizar en la fase de pre-producción (post-release).**

- Además se incluirían **costes adicionales** por **pérdida de productividad** y **confianza** por parte del cliente o usuario final.

- Un S-SDLC se ocupa desde el principio y sistemáticamente de las actividades relativas a la seguridad del software **durante todo el ciclo de desarrollo**, de manera que las vulnerabilidades y su corrección se lleven a cabo en fases incluso previas a la fase de desarrollo, reduciendo sensiblemente los costes globales del desarrollo..



Fuente: National Institute of Standards and Technology (NIST)



29 % REDUCCIÓN*

* Haciendo una equiparación del tamaño de los módulos

Fuente: Piloto implantación proyecto EOSA

Por qué un modelo de desarrollo seguro (S-SDLC)

Solución: Análisis de Metodologías y estándares de seguridad

Metodologías de Desarrollo de Software Seguro

Microsoft® Security

OpenSAMM

OWASP Open Web Application Security Project

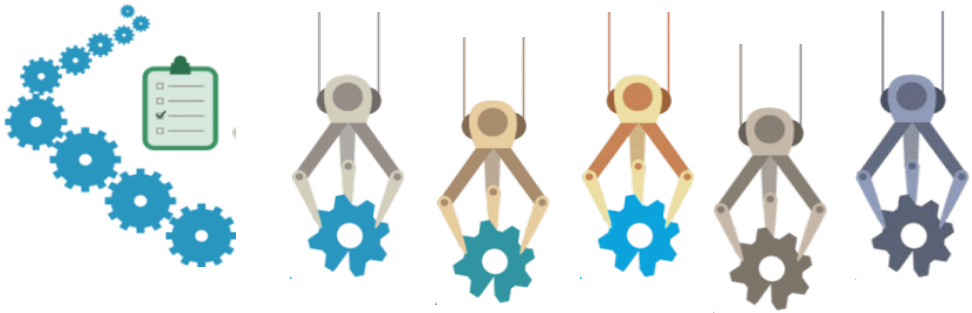
ORACLE®

BSIMM

SAFECode Software Assurance Forum for Excellence in Code Driving Security and Integrity

Software Engineering Institute Carnegie Mellon

Analizar modelos y detectar actividades recurrentes y fundamentales



Solución: Análisis de Metodologías y estándares de seguridad

Metodologías de Desarrollo de Software Seguro

METODOLOGÍA DE DESARROLLO SEGURO	EMPRESA	METODOLOGÍA
Microsoft Security Development Lifecycle	Microsoft	Tradicional
Oracle Software Security Assurance	Oracle	Tradicional
Comprehensive Lightweight Application Security Process	OWASP	Tradicional
Team Software Process Secure	Software Engineer Institute	Tradicional
Software Assurance Maturity Model	OWASP	Tradicional
Building Security In Maturity Model	Cigital	Ágil
Agile Development Using Microsoft Security Development Lifecycle	Microsoft	Ágil

Por qué un modelo de desarrollo seguro (S-SDLC)

Metodologías de Desarrollo de Software Seguro por Defecto

Microsoft® Security Development Lifecycle

Directiva obligatoria en Microsoft desde 2004:

- **Más popular y utilizado.**
- **Abundante documentación de los procesos.**

OWASP Open Web Application Security Project

OpenSAMM

Flexibilidad de aplicación empresarial

- **4 Funciones de Negocio**
- **12 Actividades de Seguridad**

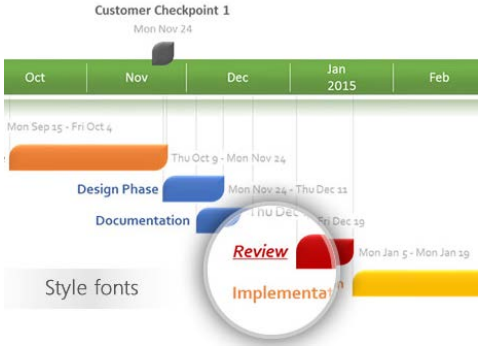
Actividades de Seguridad Identificadas

- ESTRATEGIA Y ORIENTACIÓN (Top 10 OWASP, CERT, CWE)
- FORMACIÓN EN SEGURIDAD de los grupos implicados en el desarrollo.
- Identificación y DEFINICIÓN DE RIESGOS de negocio del cliente.
- Obtención y validación de los REQUISITOS DE SEGURIDAD.
- Análisis y MODELADO DE AMENAZAS que proteja la superficie de ataques.
- REVISIÓN DEL DISEÑO.
- REVISIÓN DEL CÓDIGO.
- TESTING DE SEGURIDAD.
- VALIDACIÓN DE SALIDAS garantizando la seguridad del código liberado.
- EVALUACIÓN Y MÉTRICAS confirmando el seguimiento de la seguridad.
- Implantación de un PLAN DE RESPUESTA A INCIDENTES.

Nuevas Actividades Propuestas: Carencias detectadas de otros modelos.

Observatorio de Seguridad

Repositorio de vulnerabilidades y gestión del conocimiento



Estado del proyecto

Metamodelo de desarrollo seguro Viewnext (S-SDLC)

Estructura: Áreas de desarrollo.

Divididas en 4 Áreas de Desarrollo:

Políticas

- Definición de objetivos y directrices globales y sectoriales.
- Implicación de todos los grupos. Formación.
- Conocimiento de los riesgos.

Metodología SDL

- Construcción de software seguro por defecto:
- Requisitos, Modelado de amenazas. Diseño seguro. Análisis de código. Testing de seguridad.

Supervisión

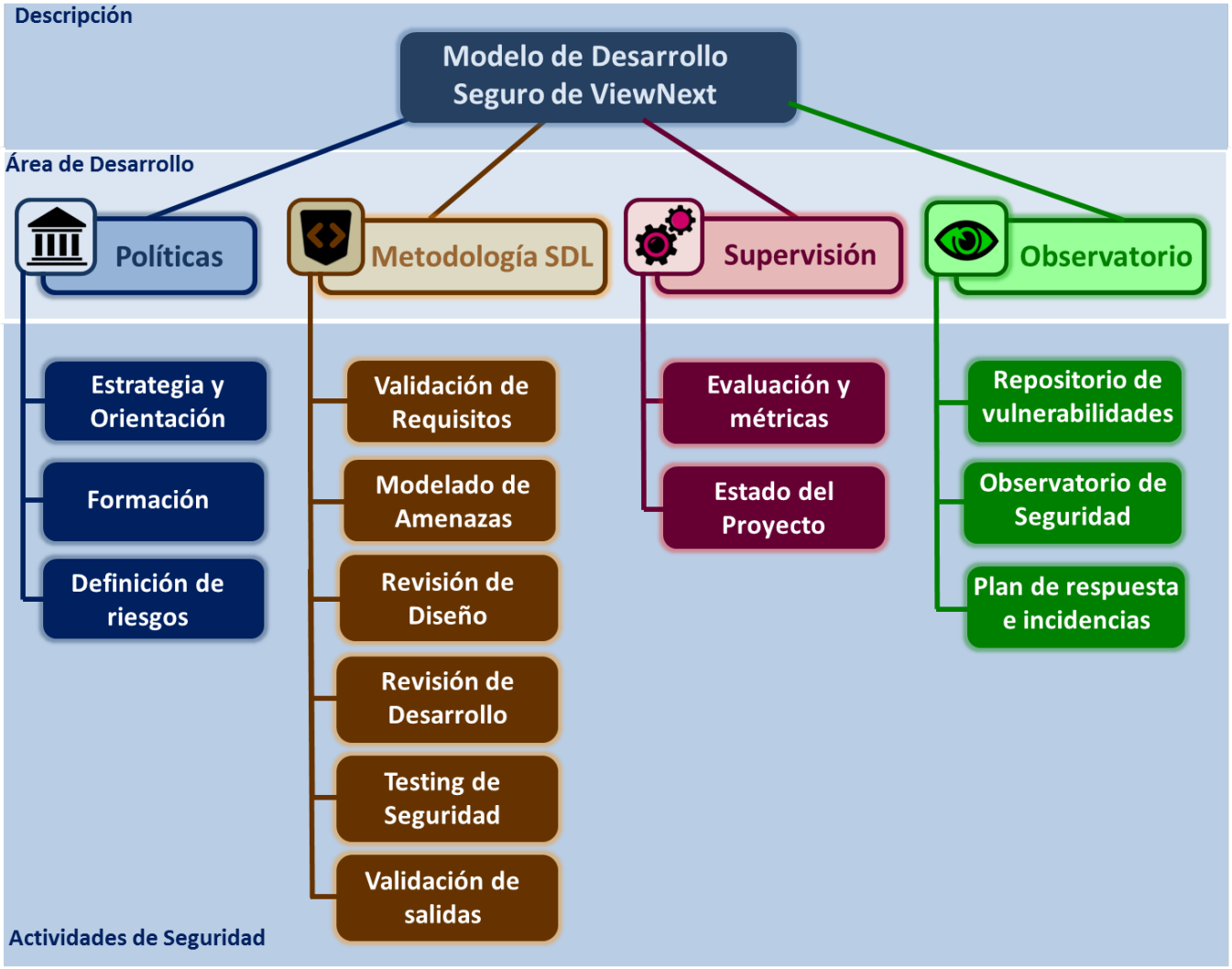
- Evaluación continua.
- Cumplimiento de seguridad.
- Conocimiento instantáneo del estado.

Observatorio

- Nuevos tipos de ataques y vulnerabilidades.
- Aprendizaje continuo.
- Convertir medidas reactivas en preventivas.

Modelo de desarrollo seguro Viewnext (S-SDLC)

Estructura Metamodelo: Actividades de seguridad



4

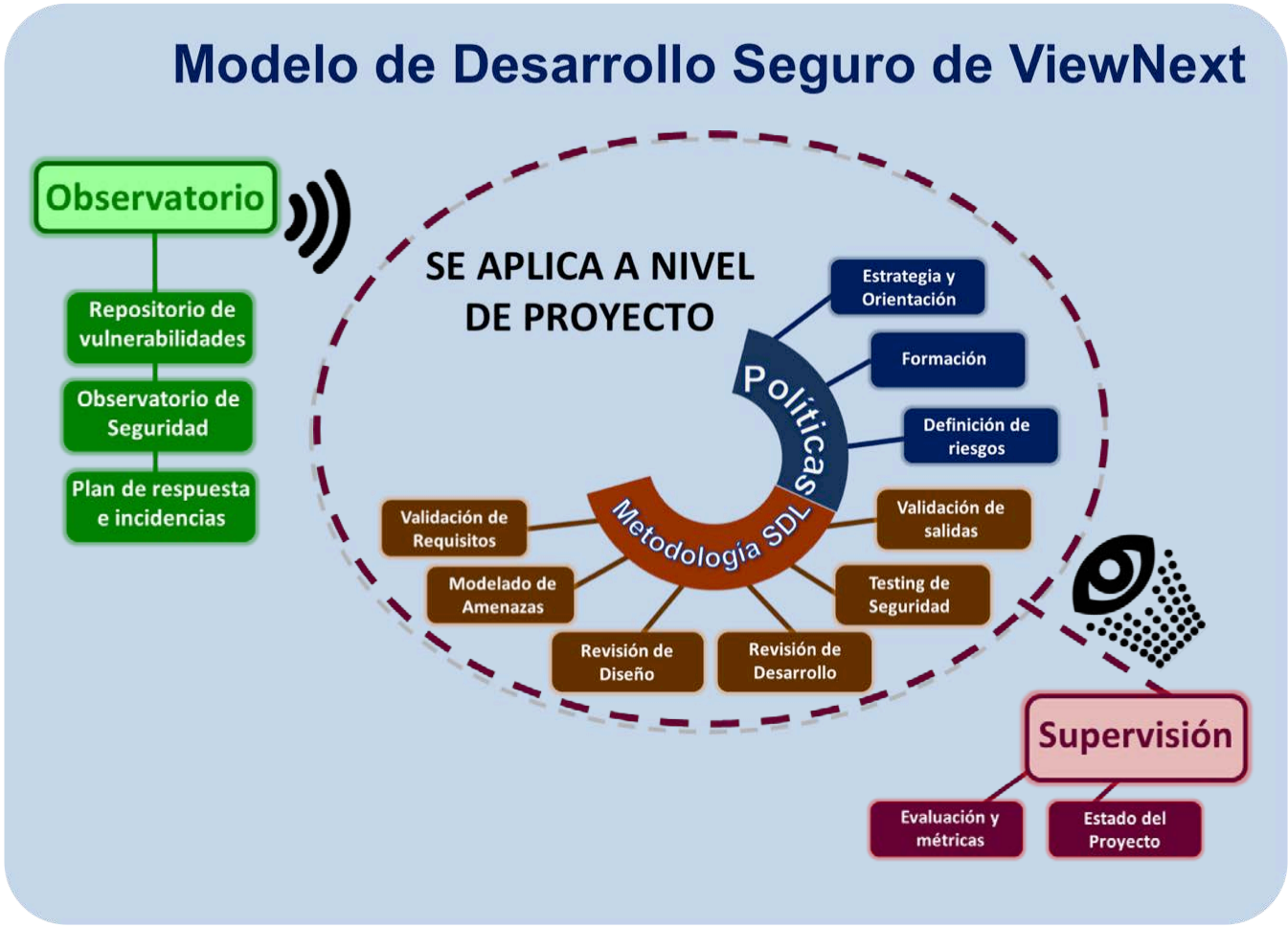
ÁREAS DE DESARROLLO

14

ACTIVIDADES DE SEGURIDAD

Modelo de desarrollo seguro Viewnext (S-SDLC)

Conexión Metamodelo: Actividades de seguridad



Políticas Metodología Supervisión Observatorio

Modelo de desarrollo seguro Viewnext (S-SDLC)

Metodología SDL: Actividades

Modelo de desarrollo seguro Viewnext (S-SDLC)

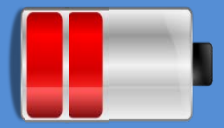
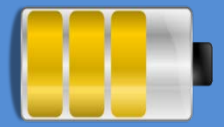
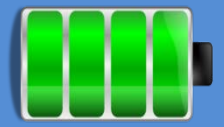
Evaluación inicial del nivel de seguridad

Proyectos con nuevos desarrollos

Proyectos en mantenimiento

Modelo de desarrollo seguro Viewnext (S-SDLC)

Niveles de Seguridad: Estándar, Moderado y Crítico.

Validación	Nivel	Descripción	Simbología
Estándar	1	Comprensión inicial y disposición específica para adoptar las actividades.	
Moderado	2	Incremento de la eficacia y eficiencia de las actividades	
Crítico	3	Realización sofisticada de las actividades acordes a un marco regulatorio específico.	

Modelo de desarrollo seguro Viewnext (S-SDLC)

Adaptaciones del modelo global Viewnext.

Metamodelo – Modelo Teórico base

TIPO DE PROYECTO	METODOLOGÍA	FASES
AMS	ÁGIL	DISEÑO TÉCNICO -> FIN
DESARROLLO 0	TRADICIONAL	ANÁLISIS FUNCIONAL->FIN

Tipología 1

- DESARROLLO 0
- SCRUM
- ANÁLISIS -> FIN

Tipología 2

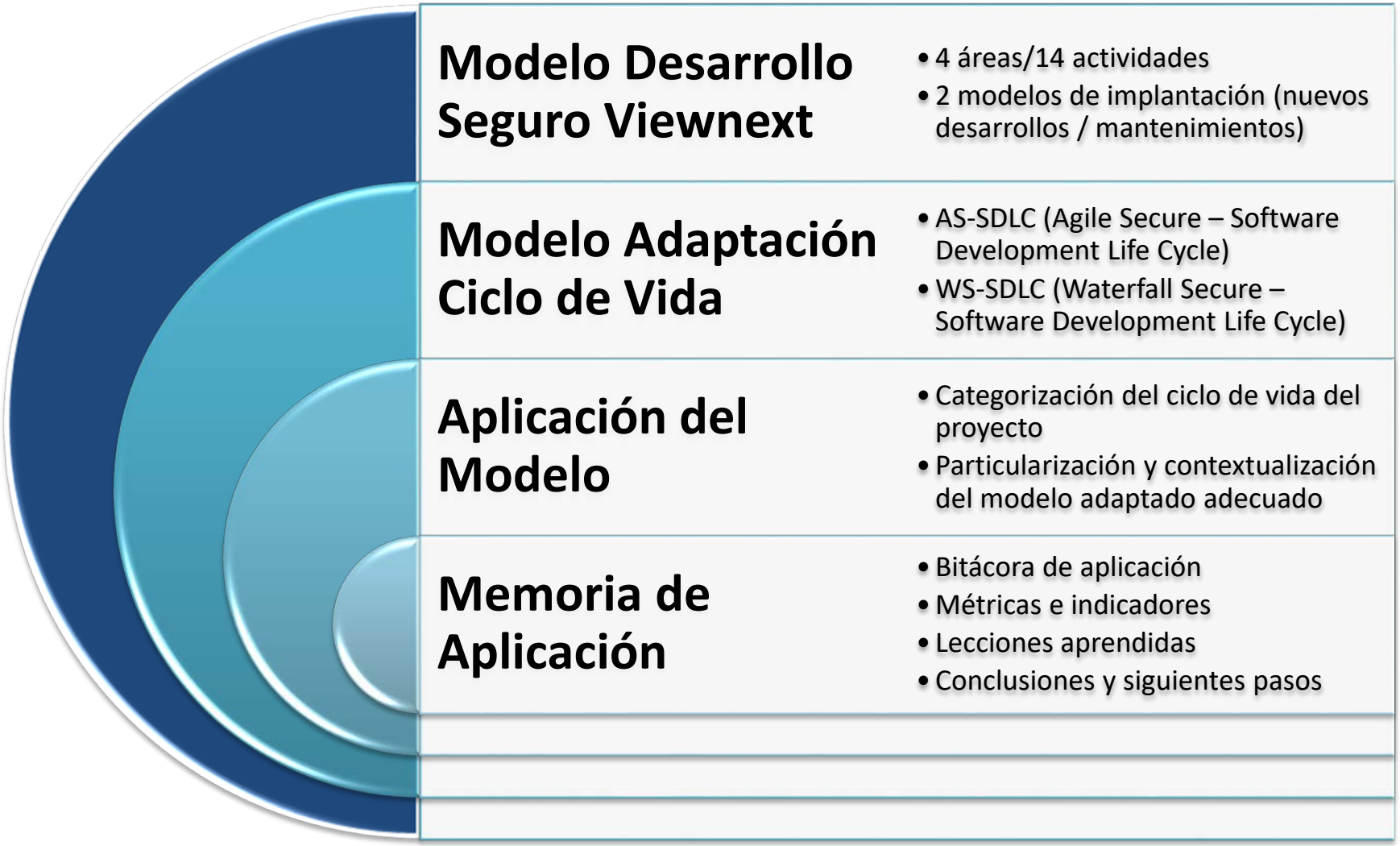
- AMS/DESARROLLO 0
- TRADICIONAL
- DISEÑO TÉCNICO-> FIN

Tipología 3

- DESARROLLO 0
- SCRUM
- DISEÑO TÉCNICO-> FIN

Modelo de desarrollo seguro Viewnext (S-SDLC)

El modelo de ciclo de vida desarrollo seguro para ADM-DW está basado en el modelo de desarrollo seguro corporativo de Viewnext, que establece 4 áreas de aplicación y 14 actividades relacionadas con la definición de un modelo preventivo, integrado e integral.



¿Cómo se implanta el S-SDLC en mi proyecto?

Metodología: 4 Fases de implantación


Cuestionario de implantación

1 **FORMACIÓN Y PREPARACIÓN DEL ECOSISTEMA**

Formación de la población

Preparación de herramientas

2 **EVALUACIÓN DE LA SEGURIDAD**

Equipo de Calidad y Pruebas

3 **INTEGRACIÓN DEL MODELO SDLC**

Requisitos
|
Modelado de amenazas
|
Buenas prácticas

4 **RETROSPECTIVA Y MEJORA CONTINUA**


Formación y Definición de indicadores de seguridad

Evaluación inicial de seguridad

Medición del coste de solucionar fallos

Integración Modelo de Desarrollo Seguro

Aplicación metodología SDL

Medición coste metodología SDL

Contrastar nivel de seguridad

Optimización del Modelo de Desarrollo Seguro

¿Cómo se implanta el S-SDLC en mi proyecto?

Metodología: Fases en las que más interviene ADM DW.

1 FORMACIÓN Y PREPARACIÓN DEL ECOSISTEMA

FORMACIÓN (EQUIPO COMPLETO)

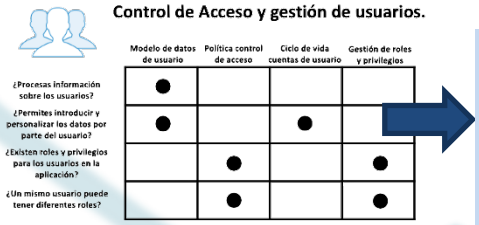
Analista de Negocio | Diseñador | Desarrollador

ECOSISTEMA DE SEGURIDAD

REDMINE, JIRA, RTC, sonarqube, BURPSUITE PROFESSIONAL

2 INTEGRACIÓN DEL MODELO SDLC

Requisitos -> Amenazas -> Prácticas seguras de codificación



Definición exhaustiva de:
– Tipos de usuario y sus privilegios.
– Ciclo de vida de los privilegios.
– Principio del mínimo privilegio.
– Fallar seguro ante escalada de privilegios.

3 RETROSPECTIVA Y MEJORA CONTINUA

Riesgo de Exposición
|
Nivel de Riesgo
|
Análisis y resolución de vulnerabilidades
|
Nivel de inversión

¿Cómo se implanta el S-SDLC en mi proyecto?

Metodología: Trazabilidad de Requisitos – Amenazas – Buenas prácticas.

Responder un cuestionario básico

¿Qué tipo de aplicativo es?

- Aplicación Web.
- Web Service.
- Aplicación móvil.

Identificar temas de seguridad

¿El sitio web requiere autenticación?

- Si.
  - Registro del estado de las operaciones de autenticación.
- No, existe funcionalidad para perfiles públicos.

¿Cómo se autentica el usuario?

- Usuario y contraseña
  - Login de sesión y criterios de contraseña segura.
- Doble factor de autenticación.
- Certificado Digital.
- Sin autenticar.

¿Se almacenan los estados de las peticiones de autenticación en un Log?

- Se almacenan sólo los intentos fallidos para su posterior análisis.

¿Existe una política de directiva de grupos - GPO (Group Policy Object)?

- Cumplir criterios de contraseña segura.
- Temporalidad (cambiar contraseñas cada dos meses.)
- Imposibilidad de repetir la misma contraseña.

Política de Control de Acceso. Autenticación

	MODELO DE DATOS DE USUARIO	POLÍTICA CONTROL DE ACCESO	ADMINISTRACIÓN DE SESIONES	REGISTRO DE OPERACIONES
¿El sitio requiere autenticación?		●	●	
¿Cómo se autentica el usuario?	●	●		
¿Log actualizado con el estado de las peticiones de autenticación?		●		●
¿Existe una política de directiva de grupos - GPO (Group Policy Object)?	●	●	●	

MODELADO DE AMENAZAS

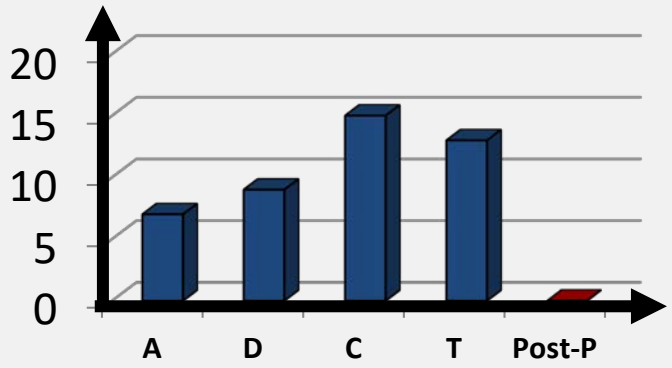
IDENTIFICACIÓN DE:

- **ACTIVOS.**
- **ENTIDADES EXTERNAS.**
- **PUNTOS DE ENTRADA.**

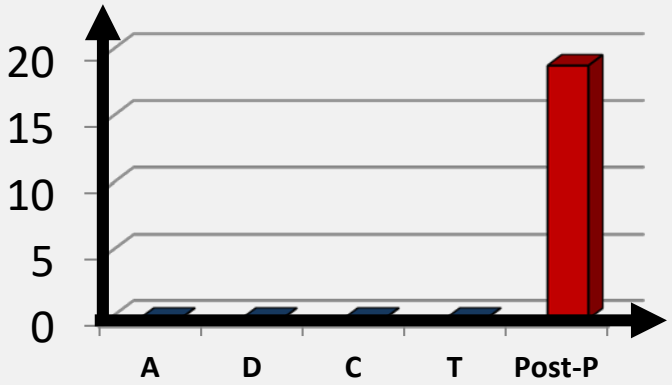
Resultado final

Comparativa de costes VS nivel de seguridad

PROYECTO SIN SEGURIDAD

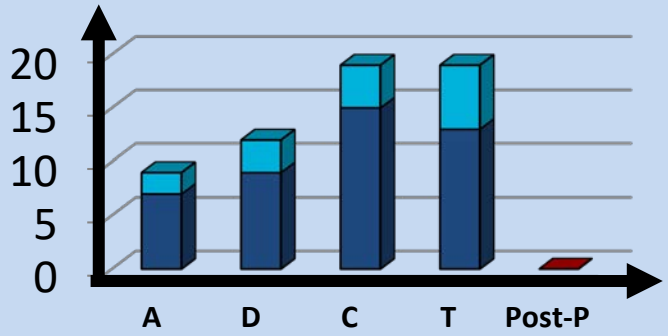


Coste por fase sin aplicar seguridad

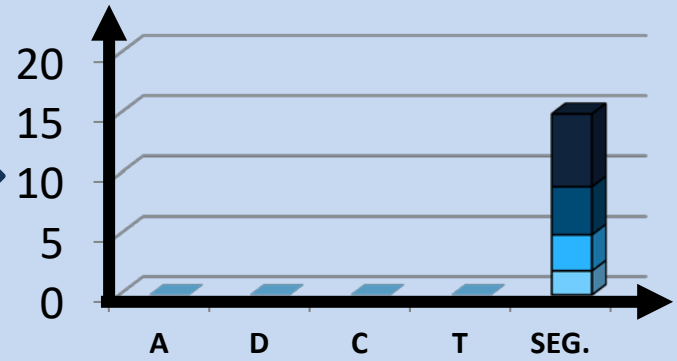


Coste corrección de vulnerabilidades

PROYECTO CON MODELO SDLC



Coste por fase con seguridad



Coste de seguridad global

Implantación Modelo de Desarrollo Seguro en Viewnext

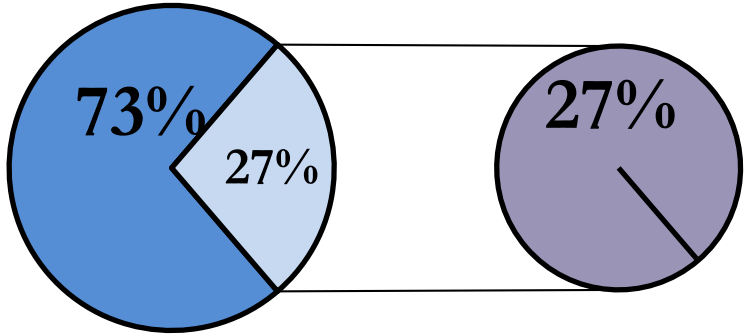
Proyecto Piloto EOSA: Contexto

- **Tipología 1**
  - DESARROLLO 0
  - SCRUM
  - ANÁLISIS -> FIN

Nuevos Desarrollos con intervención desde la fase de toma de requisitos y análisis funcional. Metodología ágil SCRUM (ciclos de liberación frecuentes).

Equipo Multifuncional

Temporalidad módulo desarrollados

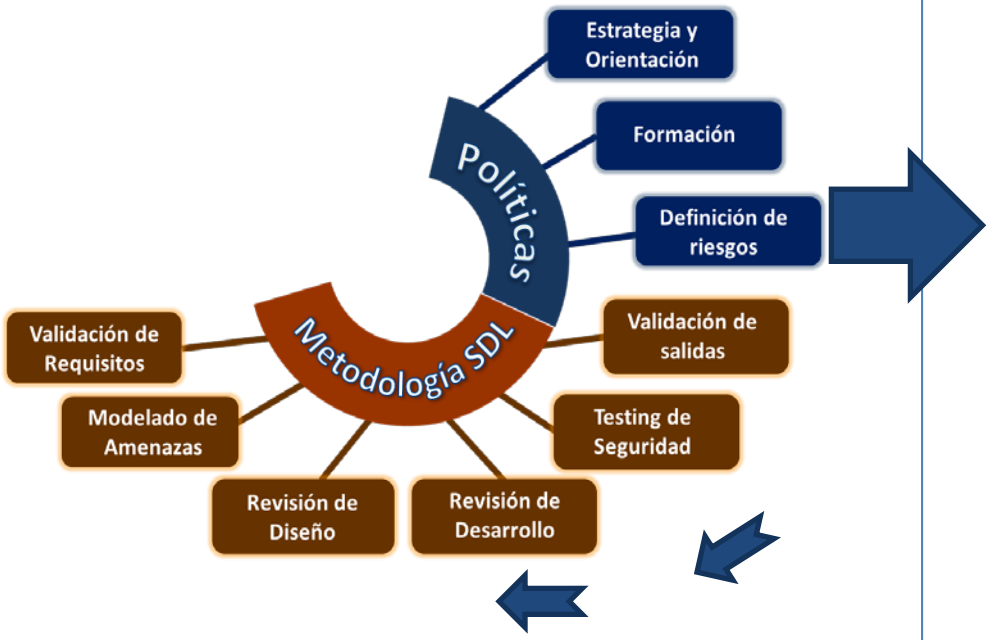


ALMACENES - 1997h **PERSONAL - 747h**

Implantación Modelo de Desarrollo Seguro en Viewnext

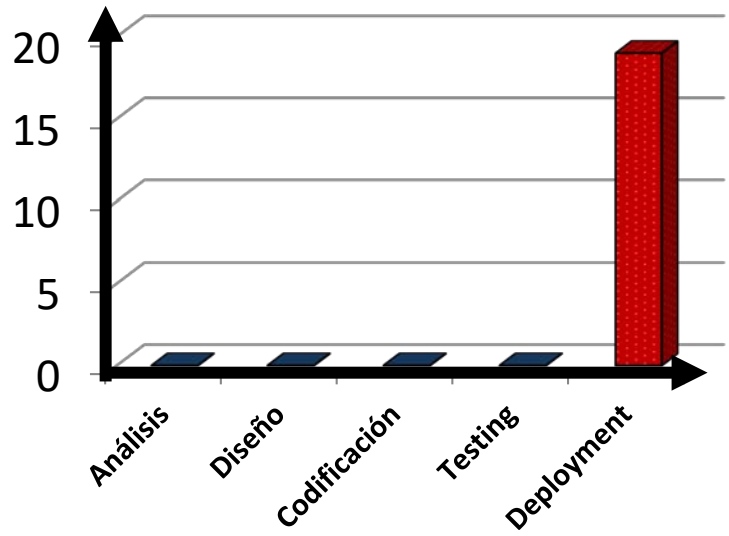
EOSA: Fase 2 - Auditoria y resolución de fallos de seguridad - ALMACENES

Proyectos en mantenimiento



Aplicar testing de seguridad y revisión de código

Detectar fallos de seguridad

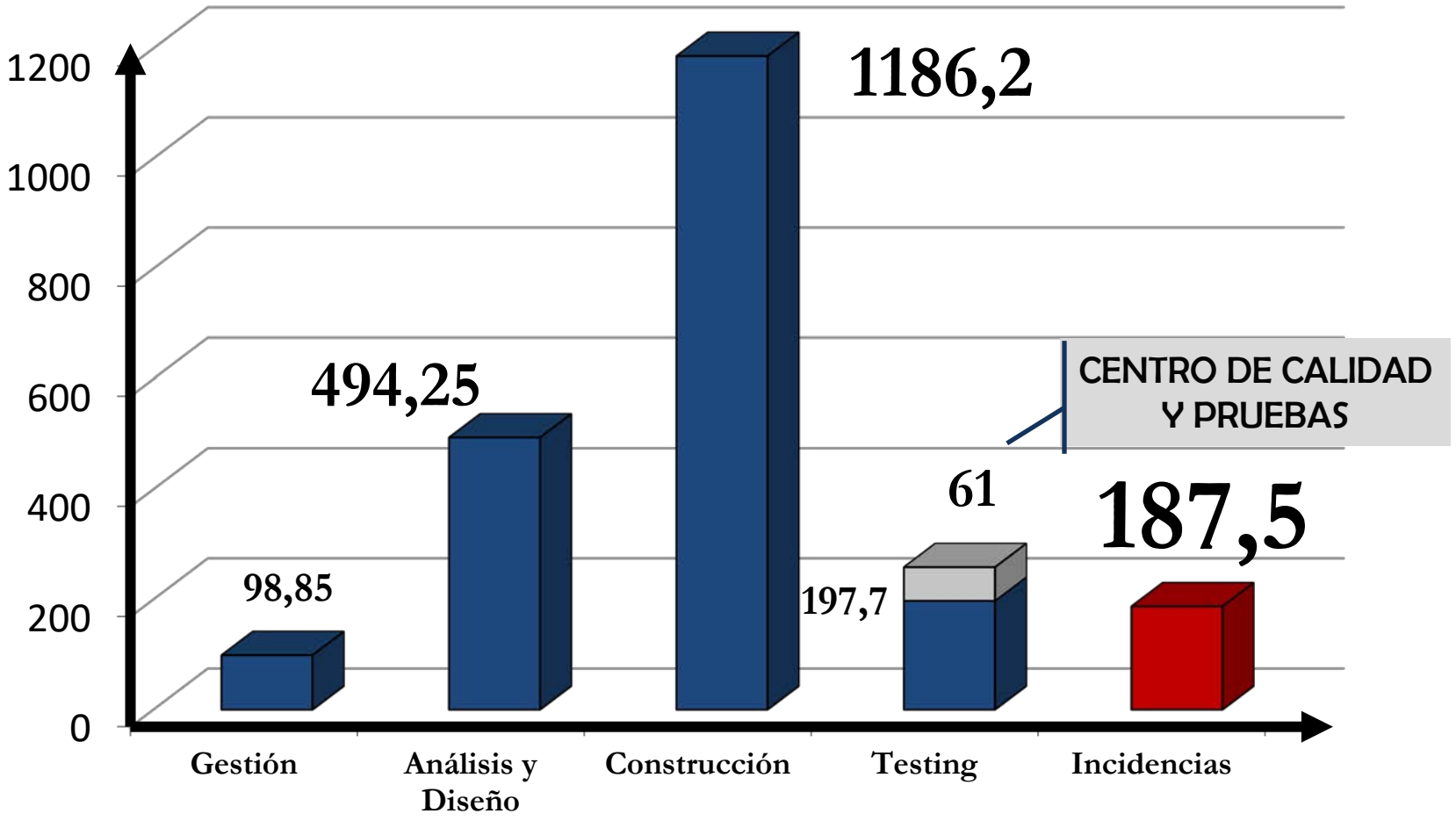


Coste resolver las vulnerabilidades

Implantación Modelo de Desarrollo Seguro en Viewnext

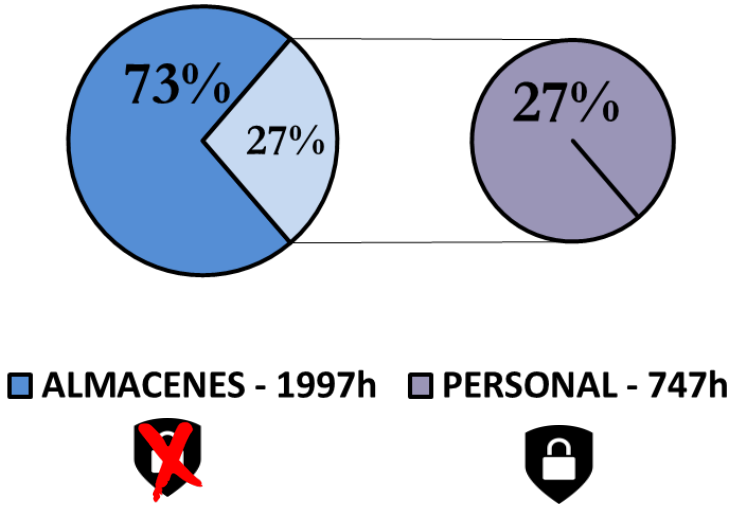
EOSA: Fase 2 - Auditoria y resolución de fallos de seguridad - ALMACENES

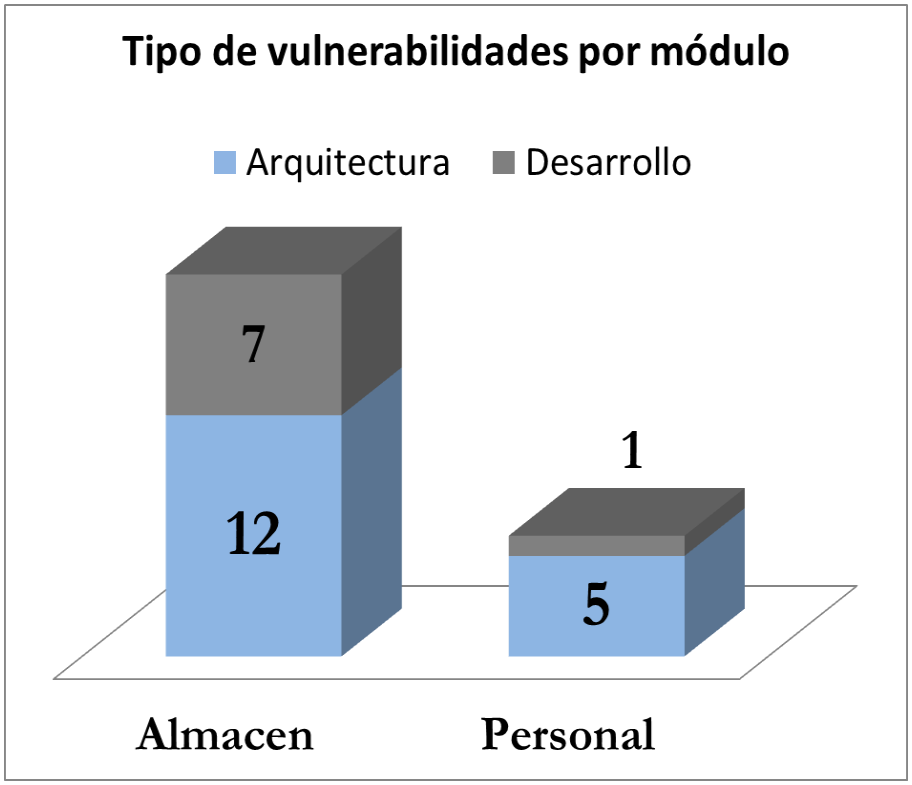
Auditoria y resolución de fallos de seguridad (horas/fase)



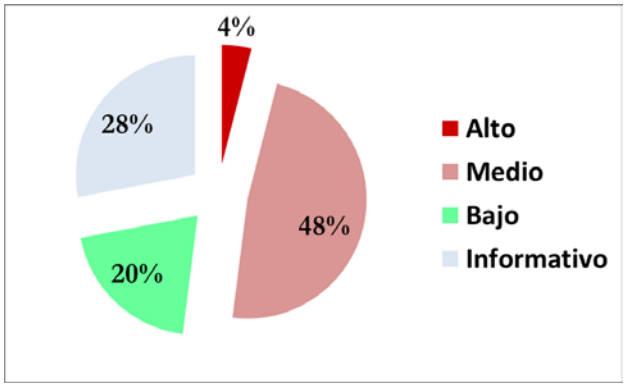
25 vulnerabilidades DAST

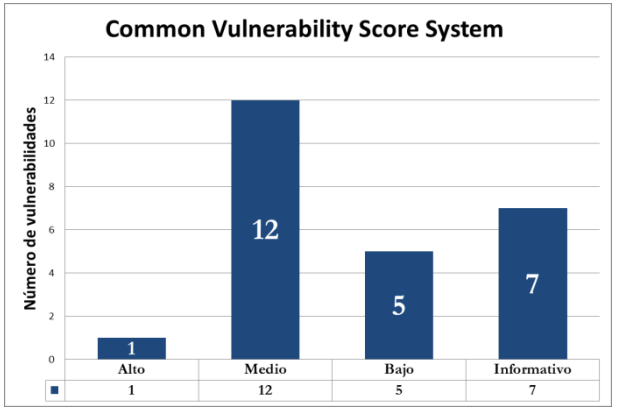
Tipos y categorías de vulnerabilidades

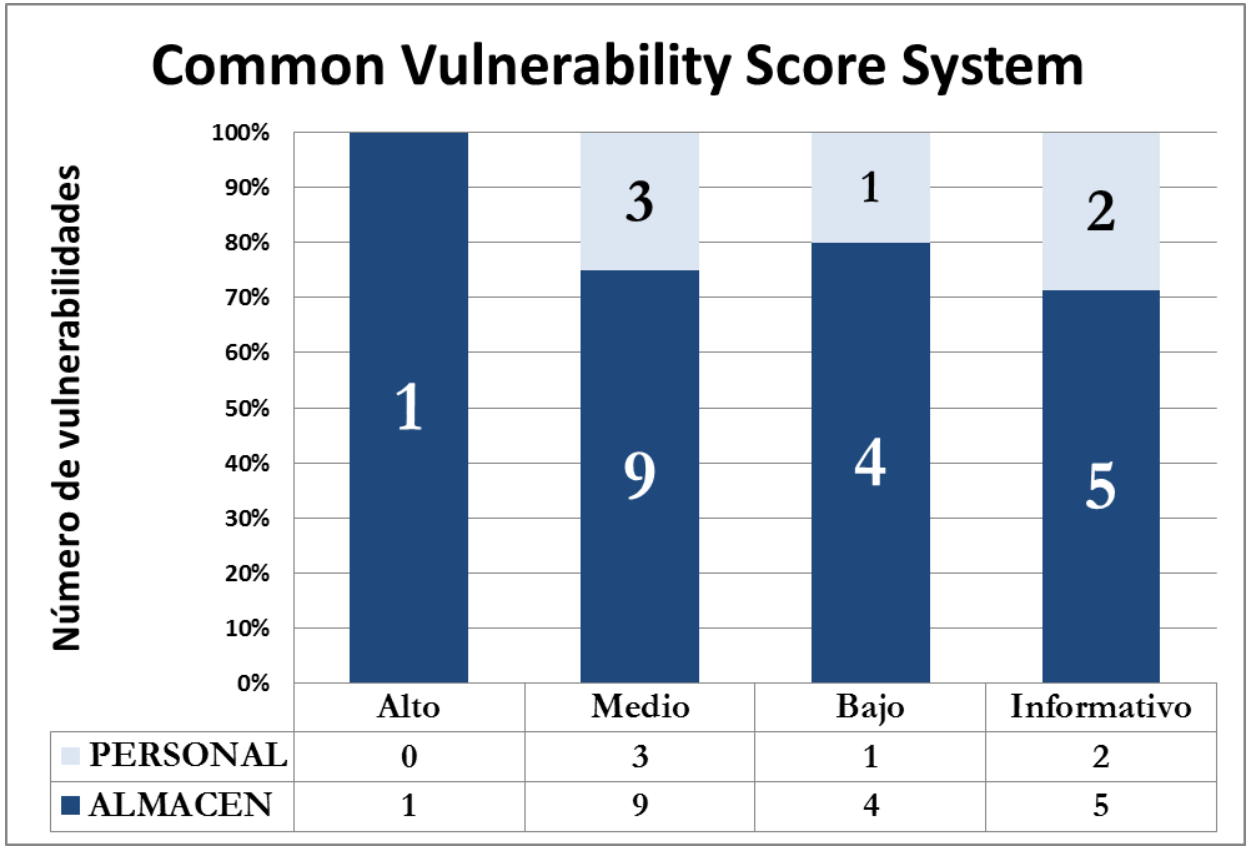




Riesgo de vulnerabilidades por módulo



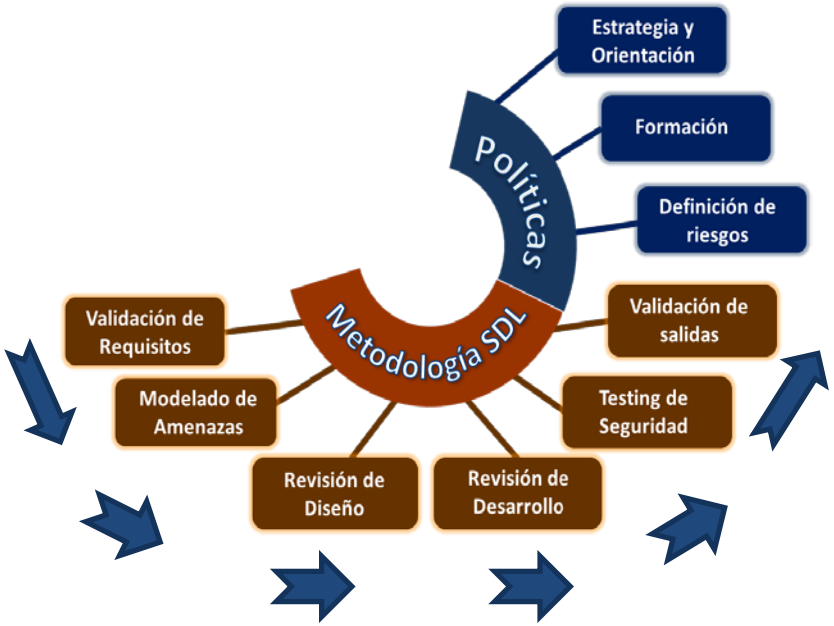




Implantación Modelo de Desarrollo Seguro en Viewnext

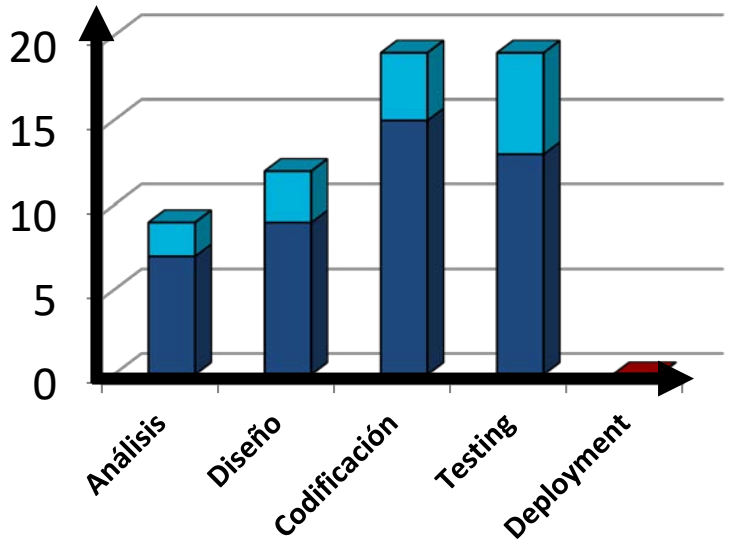
EOSA: Fase 3 - Implantación de actividades y coste - PERSONAL

Implantación en nuevos desarrollos



Aplicar la seguridad en todo el proceso de construcción del software

Incremento de coste en cada fase

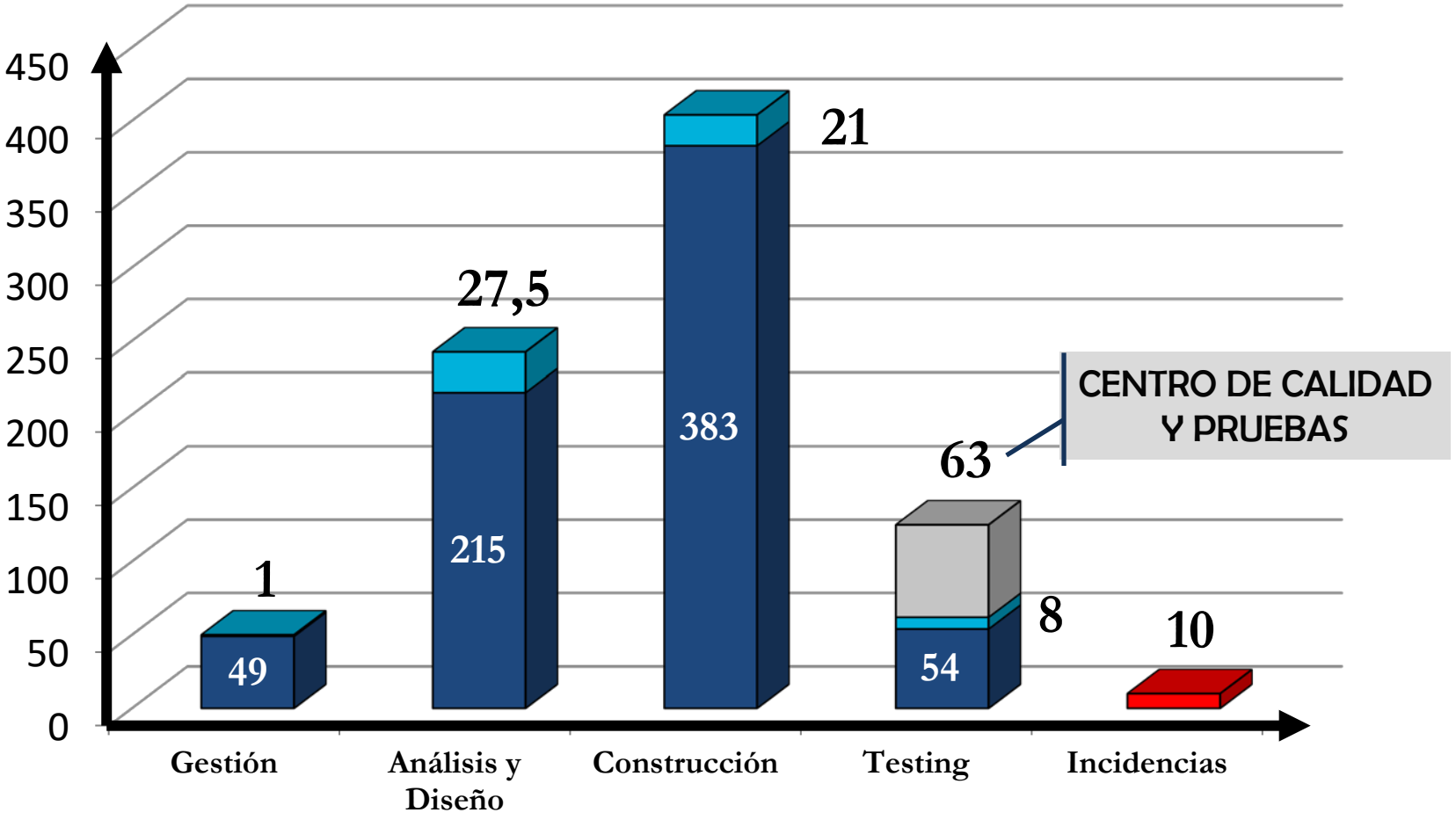


Coste por fase de aplicar seguridad

Implantación Modelo de Desarrollo Seguro en Viewnext

EOSA: Fase 3 - Implantación de actividades y coste - PERSONAL

Implantación del modelo en nuevos desarrollos e incremento de coste por cada fase



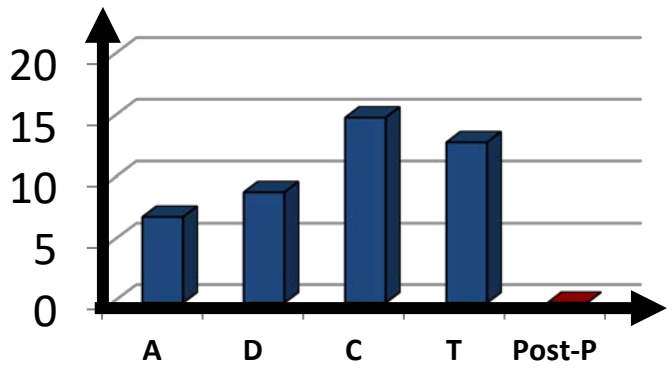
Implantación Modelo de Desarrollo Seguro en Viewnext

Proyecto Piloto EOSA: Fase 3 - Implantación de actividades y coste

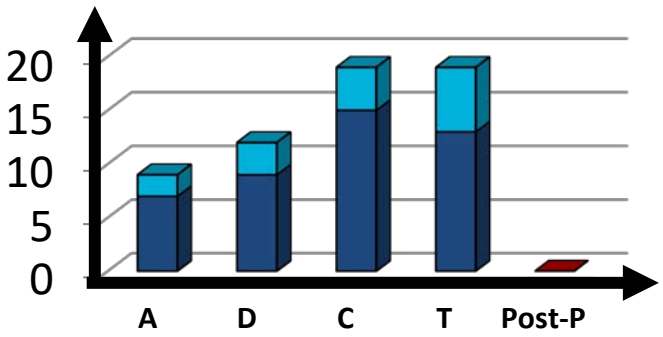
ALMACENES			PERSONAL	
Resto	Seguridad	FASE	Seguridad	Resto
99	13	GESTIÓN	1	49
494	6,5	ANÁLISIS Y DISEÑO	27,5	215,5
1186	87	DESARROLLO	21	383
198	10	TESTING	8	54
	71	INCIDENCIAS	10	
	61	AUDITORIAS	63	

Implantación Modelo de Desarrollo Seguro en Viewnext

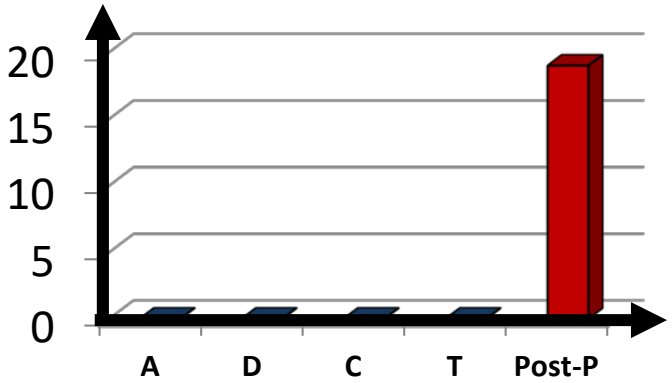
Proyecto Piloto EOSA: Fase 4 - Comparativa de costes y nivel de seguridad



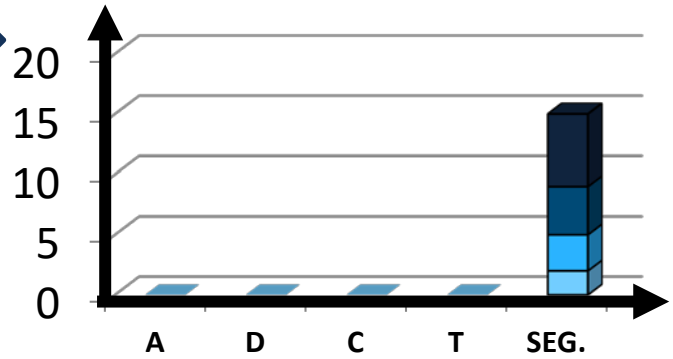
Coste por fase sin aplicar seguridad



Coste por fase con seguridad



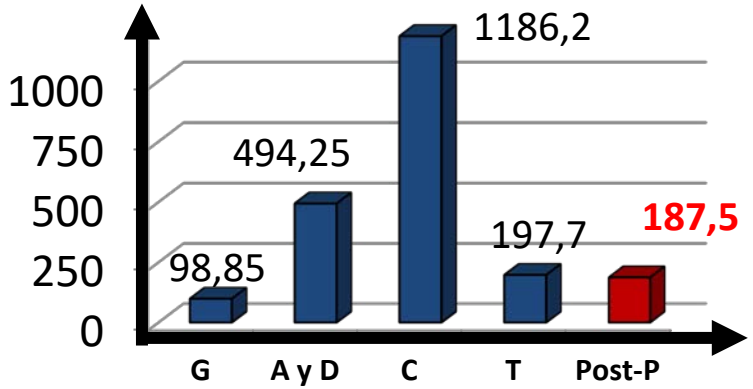
Coste corrección de vulnerabilidades



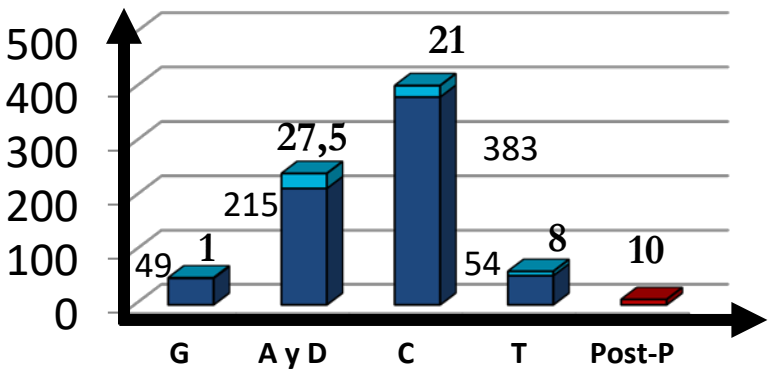
Coste de seguridad global

Implantación Modelo de Desarrollo Seguro en Viewnext

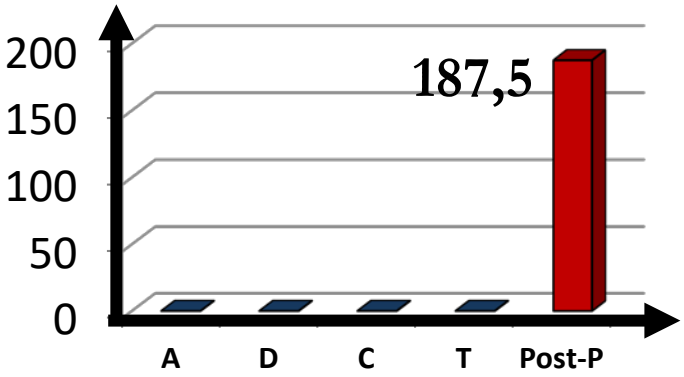
Proyecto Piloto EOSA: Fase 4 - Comparativa de costes y nivel de seguridad



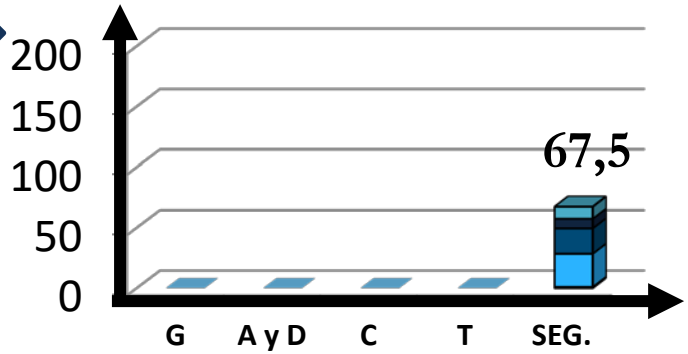
Coste por fase sin aplicar seguridad



Coste por fase con seguridad



Coste corrección de vulnerabilidades



Coste de seguridad global

Implantación Modelo de Desarrollo Seguro en Viewnext

Proyecto Piloto EOSA: Conclusiones de auditoría

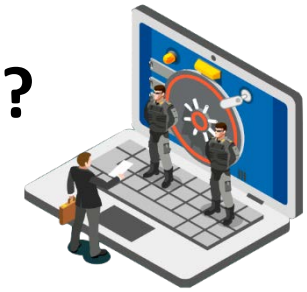
- **Dedicando mayor atención en la fase de análisis, reducimos drásticamente el tiempo de desarrollo, no así el de diseño y pruebas.**
- **Dedicando atención en la toma de requisitos, concienciamos al cliente para poder dedicar tiempo en esta área de desarrollo que da por cubierta, erróneamente, en la mayoría de los casos.**
- **El análisis de código estático es fácil de corregir, no así el manual que puede requerir incluso cambios arquitectónicos.**
- **Menor impacto y mayor seguridad al incorporar el desarrollo seguro en fases tempranas del desarrollo.**

Implantación Modelo de Desarrollo Seguro en Viewnext

Proyecto Piloto EOSA: Conclusiones de equipo

- **Incremento en la conciencia de la necesidad de un desarrollo seguro.**
- **Impacto temporal en la resolución de vulnerabilidades cuando se detectan en fases avanzadas del desarrollo y en los módulos que no han contemplado la seguridad.**
- **Contraprestaciones – Inversión adicional por parte del equipo para la implantación y adopción inicial del modelo.**
- **Incertidumbre sobre los módulos desarrollados sin tener en cuenta la seguridad.**

¿Cuándo replantearme la aplicación de un SDLC?



Si…

- Has tenido incidentes de seguridad o has actuado de forma reactiva. 1
- Es una demanda interna o existe alguna normativa de seguridad. 1
- Es una exigencia del sector de negocio. 1
- Existe un marco regulatorio sobre ciberseguridad. 1
- Lo propongo al cliente como una mejora u objetivo estratégico. 1
- Aporta ventaja competitiva al negocio. 1
- Tengo la capacidad de inversión. + 1

¿Has sumado 1 o más?

REPLANTÉATE UN S-SDLC.

GRACIAS POR SU ATENCIÓN