ONTI
Oficina Nacional de
Tecnologías de Información

Consideraciones importantes para la Seguridad de Aplicaciones

Guía Rápida

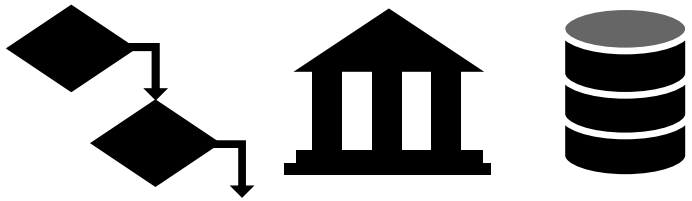
Feb 2019

NUESTRA APLICACIÓN *VA A SER ATACADA.*

ALGÚN ATAQUE *FUNCIONARÁ*.

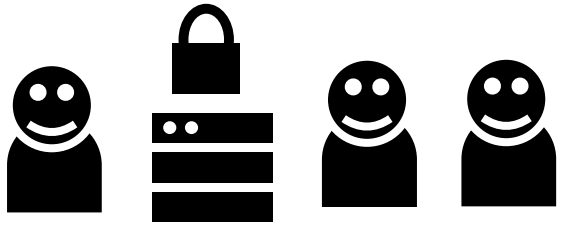
CADA DECISIÓN CAMBIA
EL NIVEL DE SEGURIDAD
DE NUESTRA APLICACIÓN

Consideración Inicial



¿Qué está en juego?

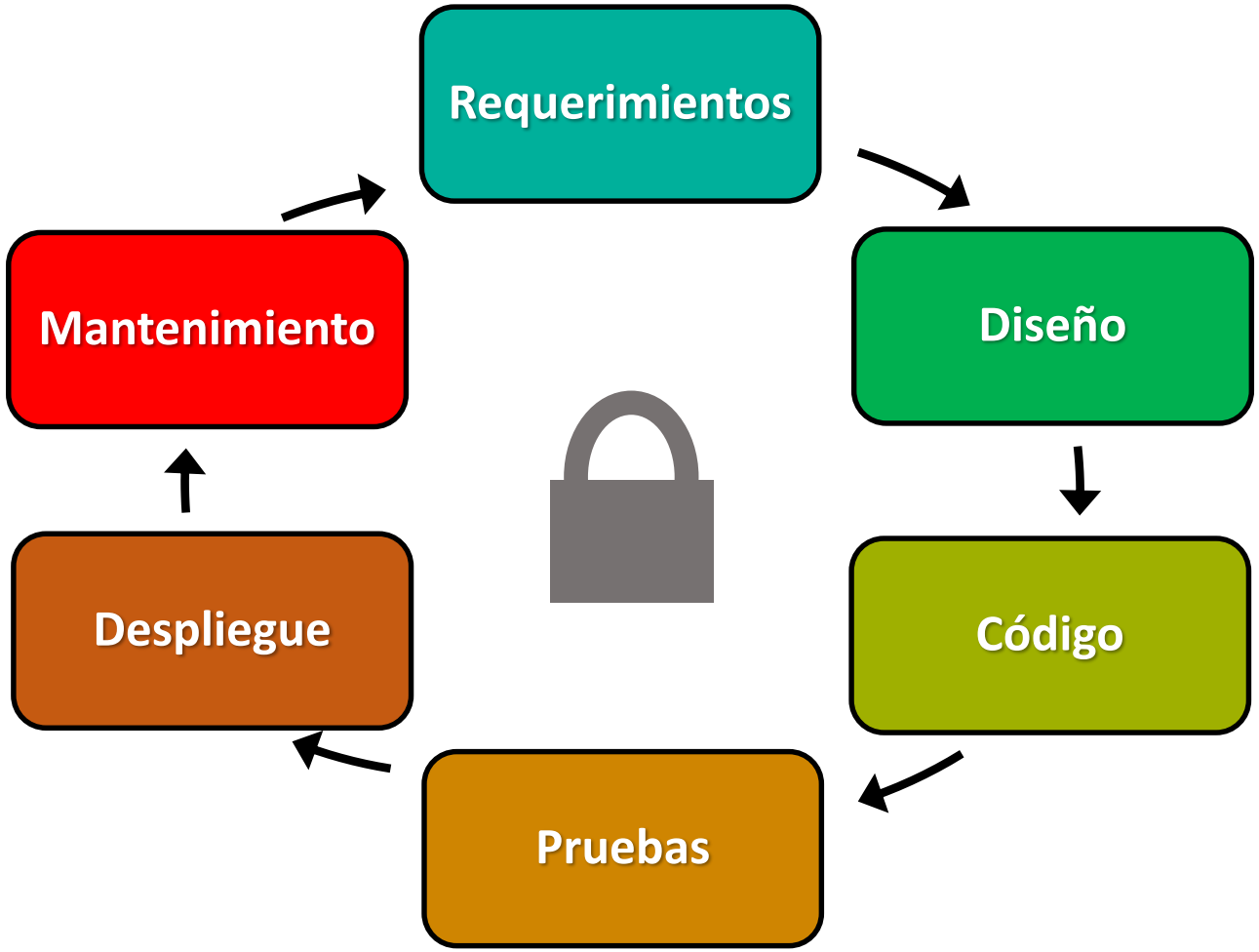
Procesos – Reputación - Activos



Involucremos a las Partes.

Equipo de Seguridad - Stakeholders

Seguridad desde el comienzo

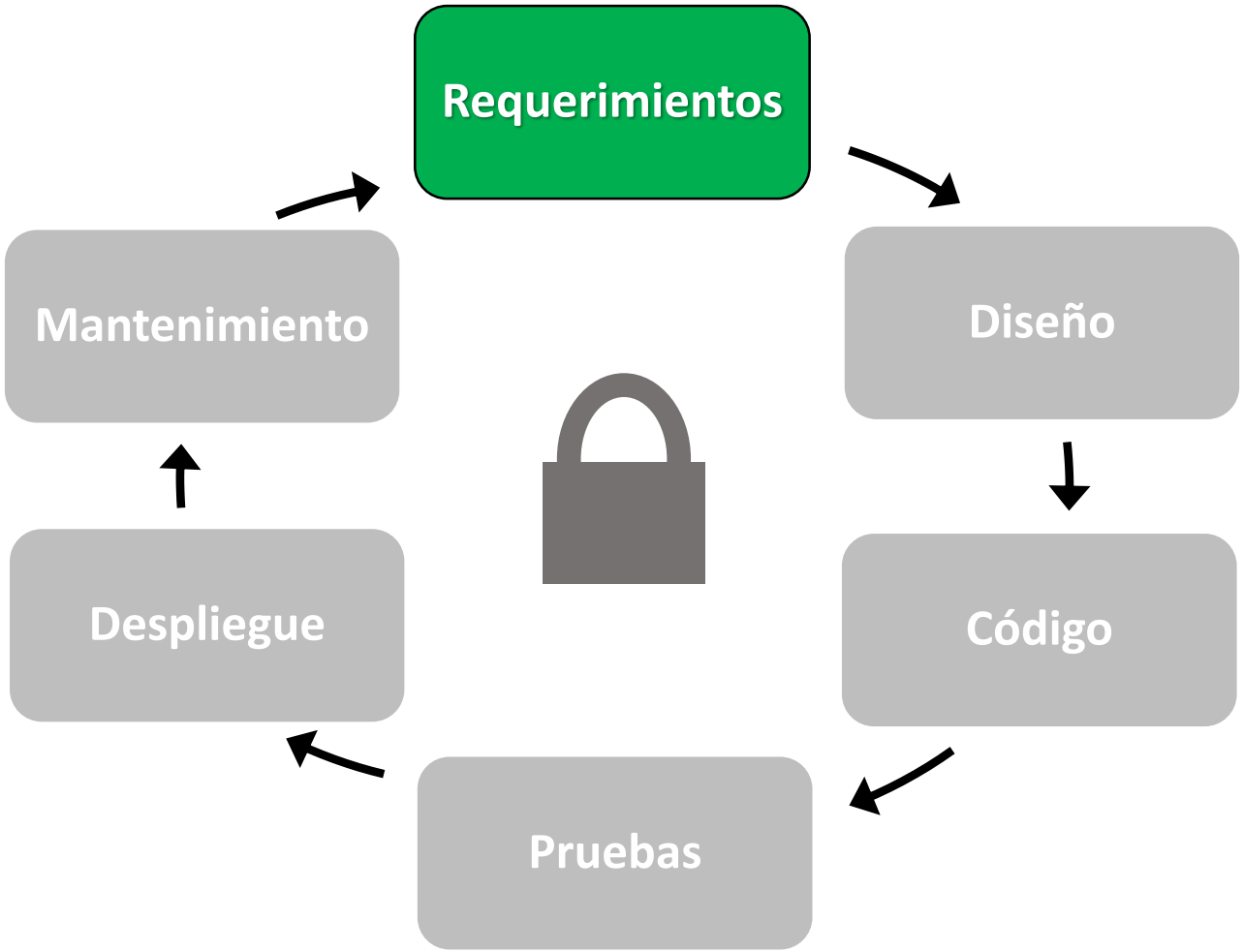


Ventajas:

Más Fácil Hacer ***Cambios***

Ciclos más rápidos

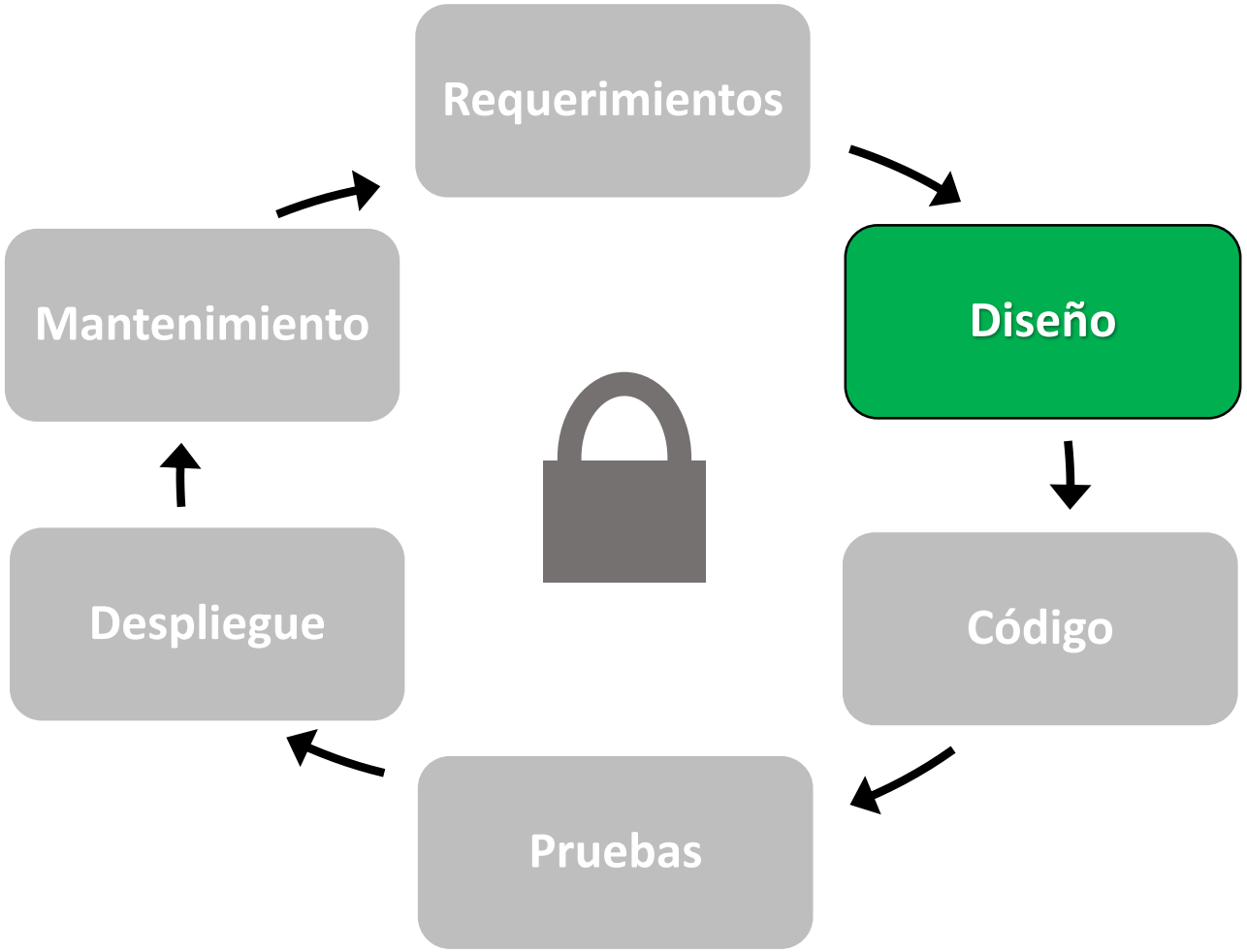
Menos Vulnerabilidades
Llegan a Producción


Requerimientos
Diseño
Código
Pruebas
Despliegue
Mantenimiento

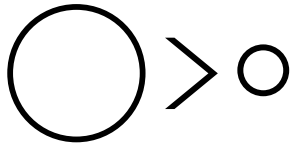
Requerimientos y Seguridad

Información de los Usuarios	1. Requerimientos de Privacidad
Riesgos Innecesarios	2. Requerimientos arbitrarios
¿Qué estamos defendiendo?	3. Clasificación de Activos
¿Qué nos pueden hacer?	4. Casos de Abuso
¿Cómo nos defendemos?	5. Requerimientos de Seguridad
¿Qué llegamos a cubrir?	6. Priorización de requerimientos

Generar documentación


Requerimientos
Diseño
Código
Pruebas
Despliegue
Mantenimiento

Principios para un Diseño Seguro



Superficie de Ataque

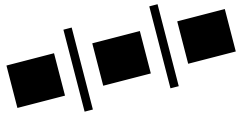
Seguridad por Defecto

Mínimo Privilegio

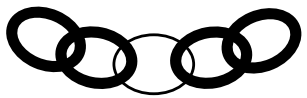
Diseñar para Mantener

UX

Mantener la Usabilidad

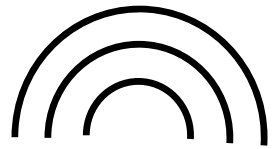


Separar Responsabilidades



El Eslabón más Débil

Diseño sin Secretos

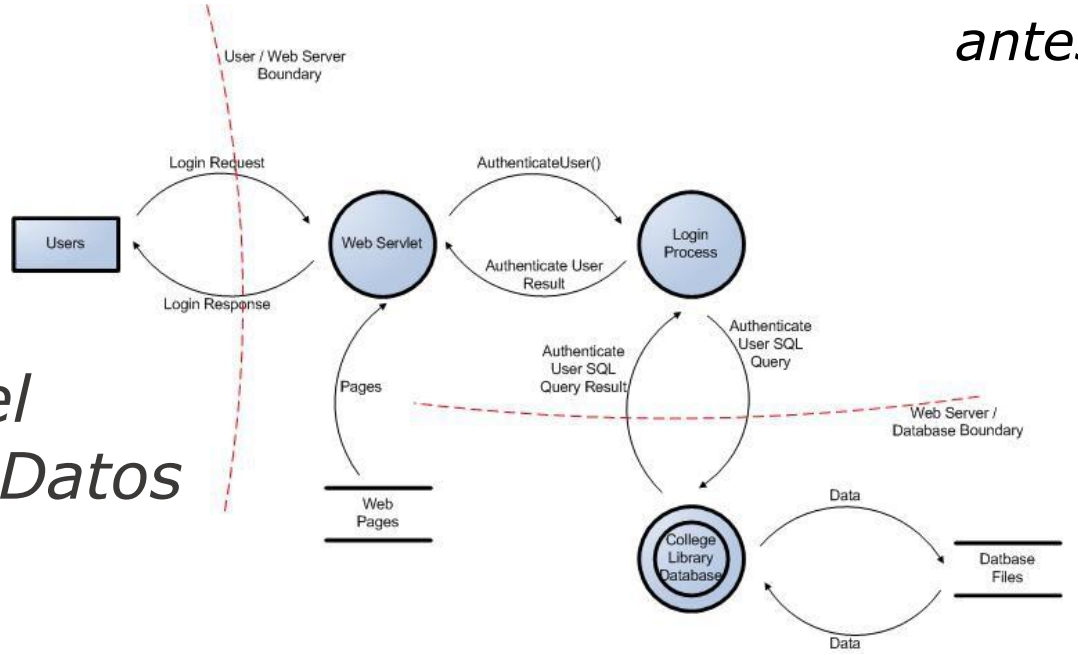


Defensa en Profundidad

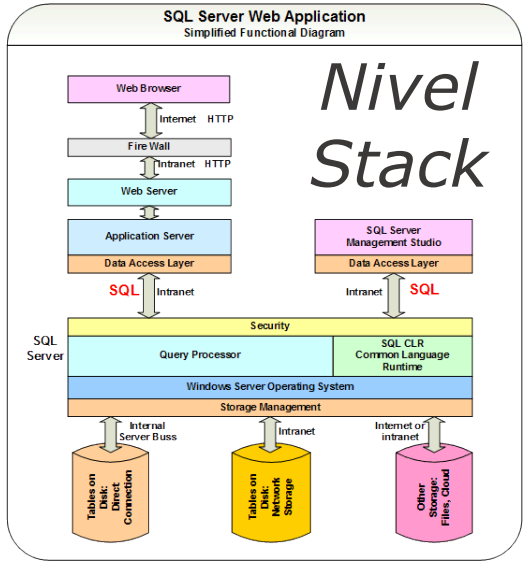
Modelado de Amenazas

Revisamos qué seguridad le falta al diseño antes de empezar la implementación

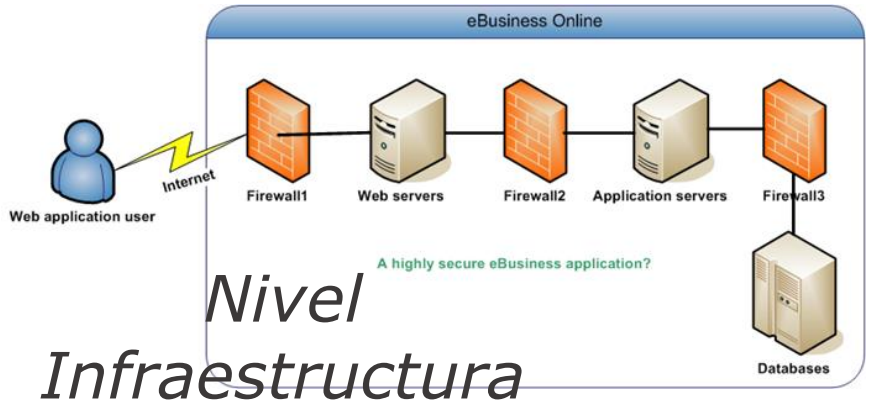
Nivel Flujo de Datos



Nivel Stack

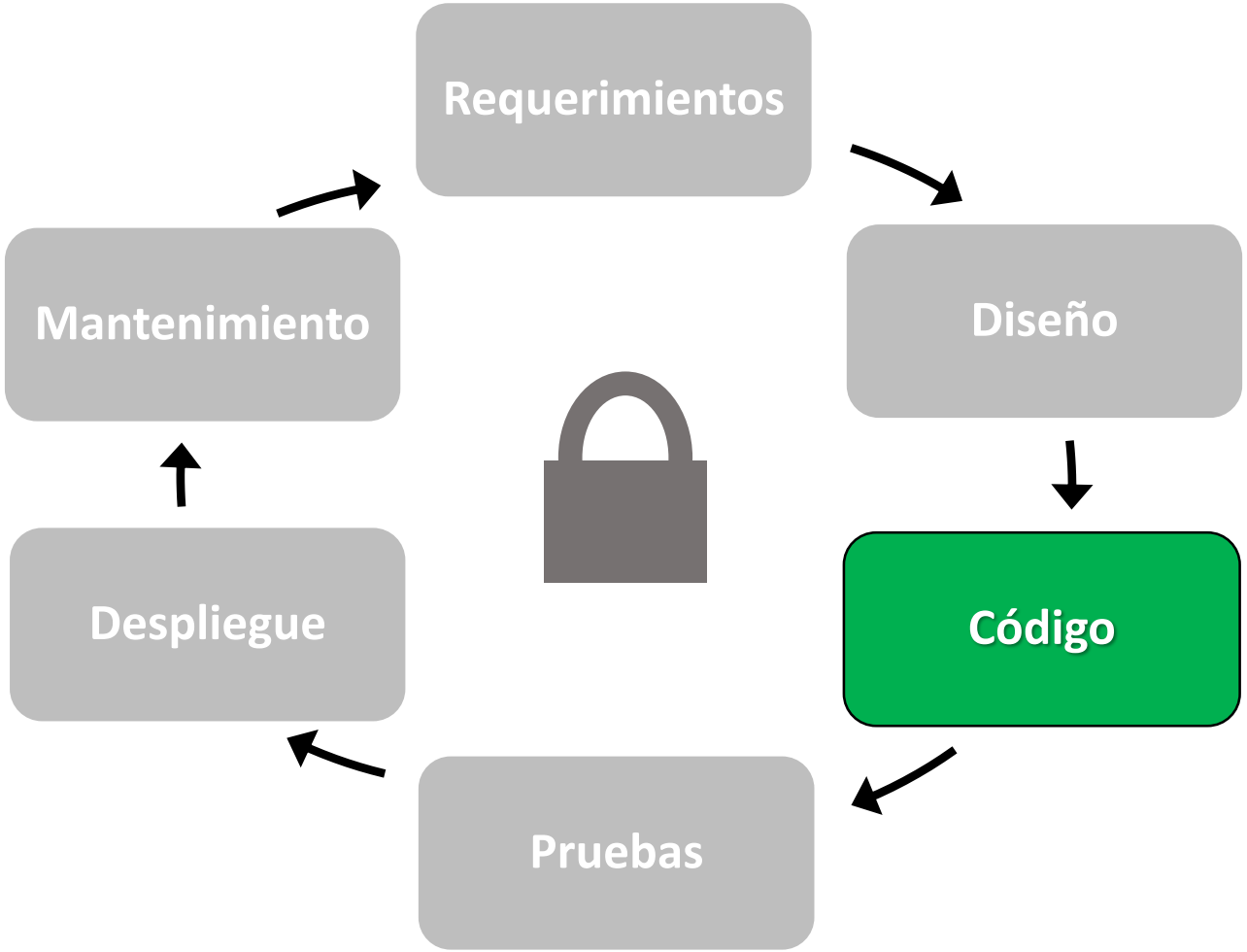


Nivel Infraestructura

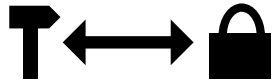


Criterios de Clasificación:

STRIDE DREAD Trike OCTAVE

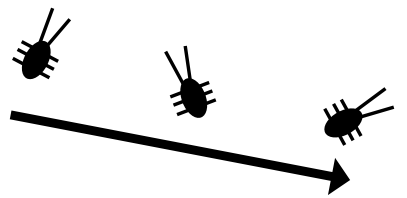

Requerimientos
Diseño
Código
Pruebas
Despliegue
Mantenimiento

Seguridad durante la Implementación

Herramientas con soporte de Seguridad 

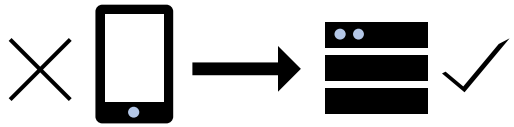
Mantenibilidad ⇔ Seguridad

Control de Versiones (auditabilidad)

Seguimiento de Bugs 

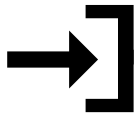
 Prudencia al reutilizar código

Seguridad de Código

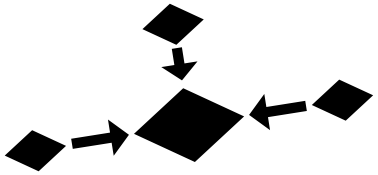


Controles en el Server

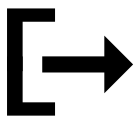
Criterio de Lista Blanca



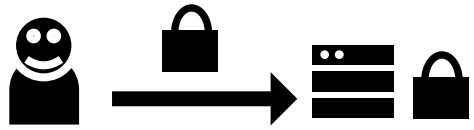
Validar todo Input



Unificar el Código de Controles

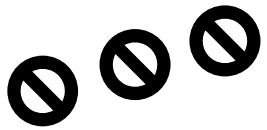


Escapar todo Output



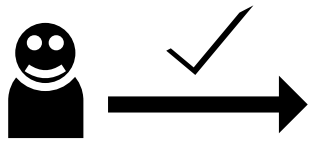
Cifrar Información de Usuarios

Seguridad de Código

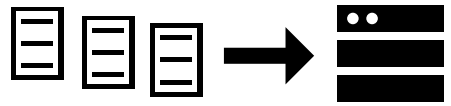


Autorización para todo por default

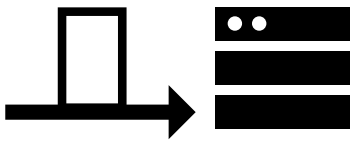
Verificar los Componentes
que elegimos usar



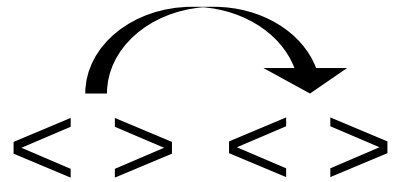
Atención al Control de Sesiones



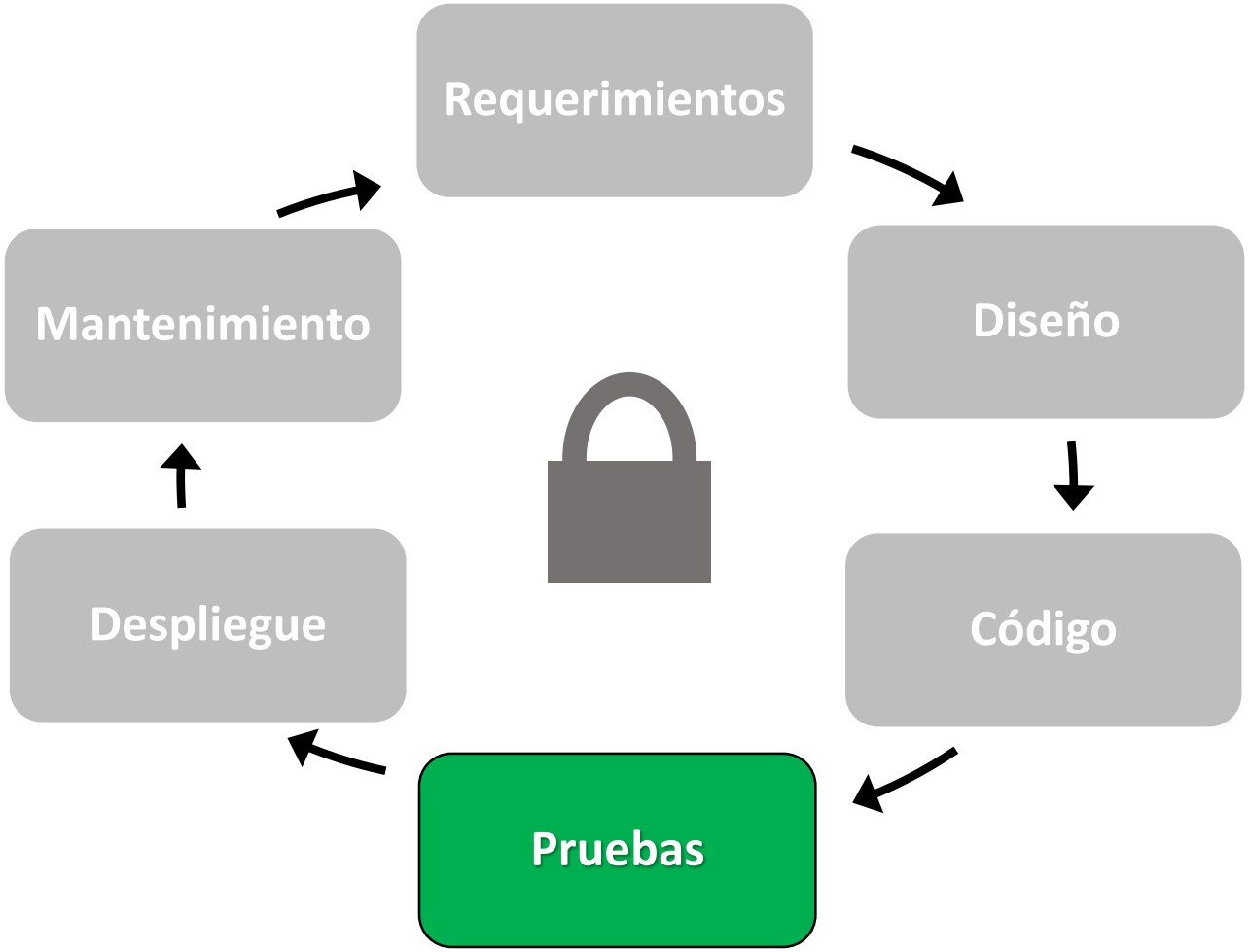
Carga de Archivos



Cuidado con los
“atajos de testing”



Integridad de Código


Requerimientos
Diseño
Código
Pruebas
Despliegue
Mantenimiento

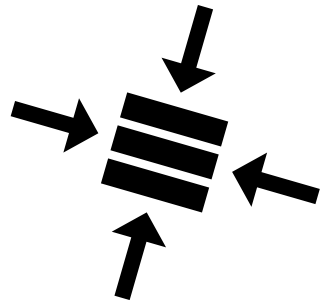
Desarrollo Basado en Pruebas

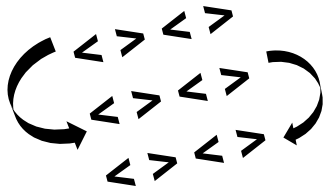
☺<>☺

Revisión de Código entre Pares

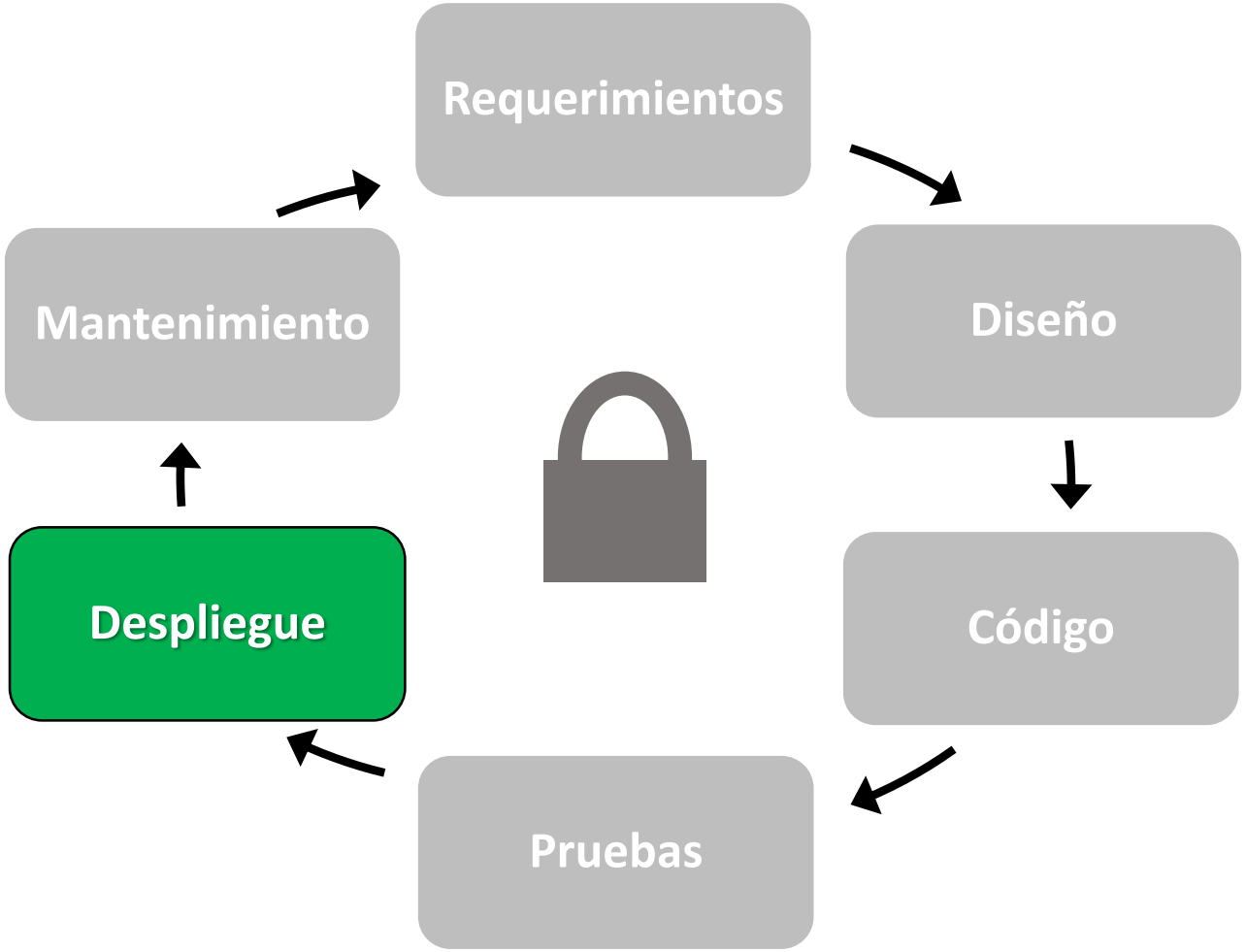
Análisis Estático: IDE / Intérprete / Framework

Pruebas de Penetración

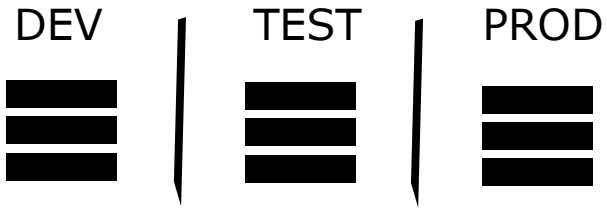




Auditorías manuales de código


Requerimientos
Diseño
Código
Pruebas
Despliegue
Mantenimiento

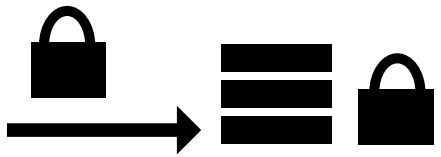
Hardenizado de Entornos



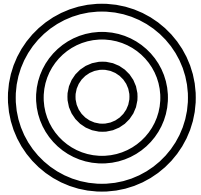
Segregación de Ambientes

Principios para Hardenizar Entornos

Quitar Componentes Innecesarios.
Configurar Bien los Necesarios.
Agregar Módulos de Seguridad.
Instalar Actualizaciones.
Documentar la Configuración.

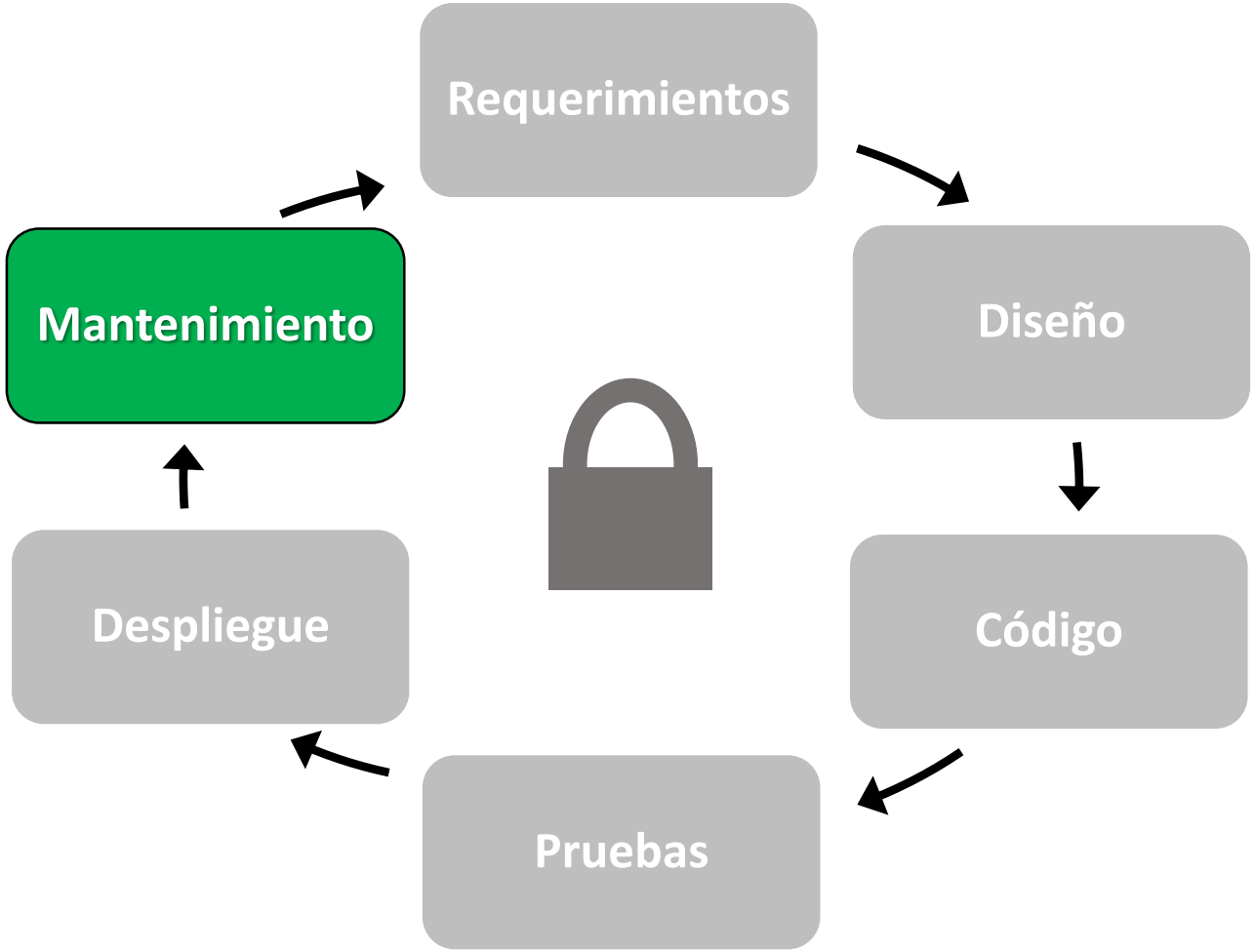


Activar Cifrado



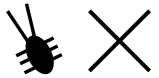
Virtualización
Y Contenedores

Cambiar Contraseñas
Por Default

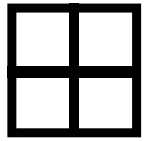

Requerimientos
Diseño
Código
Pruebas
Despliegue
Mantenimiento

Monitoreo y Mantenimiento

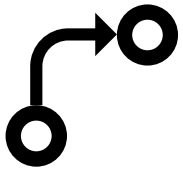
Herramientas de Seguridad



Canal de Reporte de Vulnerabilidades



Ventana de Vulnerabilidad

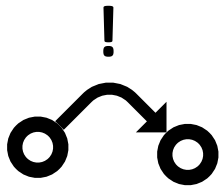


Actualizaciones Efectivas

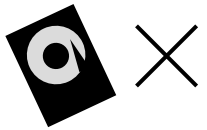
Protocolo de Backups

Controles de Integridad de código

Fin de la vida útil



Migración
Tratar datos importados como hostiles



Descarte
Validar la destrucción de los datos descartados

ONTI

Oficina Nacional de Tecnologías de Información

Secretaría de Modernización
Presidencia de la Nación