Curso de **Desarrollo Web** en **PHP orientado a objetos** con **MVC**

Eugenia Bahit, Mayo 2015

13

Seguridad Informática

Seguridad por diseño

Saneamiento de código y de datos

ADVERTENCIA

Todos los procesos de seguridad, sean tanto sobre el código como sobre los datos **deben** ser implementados una vez la funcionalidad se encuentre desarrollada pero antes de la aplicación de restricciones específicas.

FLUJO DE TRABAJO:

desarrollar → sanear → validar → restringir

No seguir el flujo de trabajo indicado generará la ofuscación de código y su consecuente dificultad de mantenimiento.

1 Saneamiento de código
en la seguridad por diseño

Consiste en probar la aplicación utilizándola de forma no esperada o indeseable. Por ejemplo, ¿qué sucede si se intenta acceder a una URL mal formada?

METODOLOGÍA DE TRABAJO

1) La aplicación debe probarse **monitorizando el log de errores** en tiempo real

```
tail -f logs/errors.log
```

2) **Se ejecuta una acción** e inmediatamente se comprueba el log de errores

3) Se toma **solo el primer error, se corrige** el código

4) **Se repite la acción** del paso 2 y se aplica el paso 3 nuevamente tanto como sea necesario

SE RECOMIENDA VER EL VIDEO SOBRE "SEGURIDAD EN EL CONTROLADOR"

2 Saneamiento de datos
en la seguridad por diseño

Se aplican diferentes tipos de filtros de saneamiento a cada uno de los datos que llegan externamente a la aplicación.

TIPOS DE FILTRO

- Eliminación:
  se eliminan caracteres innecesarios
- Conversión:
  se convierten los datos, forzadamente, al tipo necesario
- Codificación:
  se codifican los caracteres conflictivos

SE RECOMIENDA LEER EL DOCUMENTO SOBRE "SEGURIDAD POR DISEÑO"

3 Validación de datos
en la seguridad por diseño

Se valida que los datos que llegan a la aplicación cumplan con los requisitos de calidad (QA) más básicos con los que debe contar un sistema informático.

VALIDACIONES FRECUENTES

- Longitud:
  Se valida que los datos posean la longitud deseada. Se busca evitar la persistencia de datos nulos (vacíos).

- Duplicidad:
  Se validan los datos en busca de información duplicada (ya existente). Se busca evitar la persistencia de datos repetidos.

- Formato:
  - Se valida que los cumplan con el formato deseado y se les aplica dicho formato de ser necesario. Se busca evitar la persistencia de datos corruptos.

SE RECOMIENDA LEER EL DOCUMENTO SOBRE "SEGURIDAD POR DISEÑO"