Telefónica Tech

# Construyendo un futuro seguro

Implantando Secure Software Development Life Cycle

## ¿Qué es el SSDLC?

El **SSDLC** o (**Ciclo de Vida de Desarrollo de Software Seguro**) es un enfoque de desarrollo de software que integra la identificación y mitigación de vulnerabilidades a lo largo del proceso. Su objetivo es optimizar los flujos de trabajo mediante actividades específicas, lo que permite a los equipos reducir los riesgos y crear aplicaciones más resilientes frente a amenazas en constante evolución.

A diferencia del **SDLC**, que estructura y controla el proceso de desarrollo, el **SSDLC** sigue las mismas fases, pero con actividades de seguridad integradas en cada una.

## ¿Cuáles son las fases de la *implantación* del SSDLC?

### Planificación y Análisis

Identificación y evaluación de los riesgos de seguridad, mediante la creación de un modelo de amenazas y la selección de los requisitos de seguridad.

### Diseño

Integración de medidas de seguridad en el diseño, así como las pruebas de seguridad para cada fase.

### Implementación

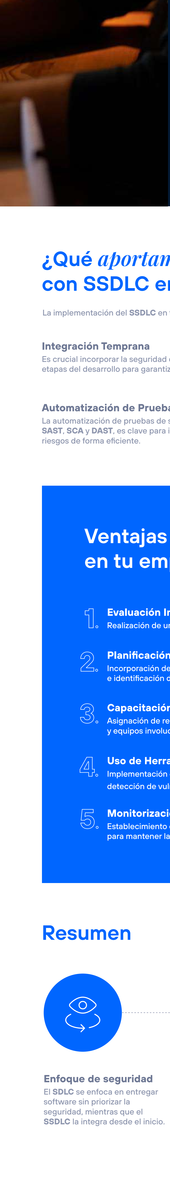
Seguimiento de directrices de codificación segura, usando herramientas de análisis para identificar y corregir vulnerabilidades durante el desarrollo.

### Pruebas

Realización de pruebas de seguridad estáticas y dinámicas para asegurar el software antes del despliegue y estableciendo Security Gates.

### Mantenimiento

Monitorización continua del software en producción, pruebas de penetración periódicas y ejecución de planes de respuesta a incidentes para gestionar riesgos emergentes.



## ¿Cuáles son los motivos para *implementar* SSDLC?

Las brechas de seguridad en el **SDLC** tradicional son graves debido a su enfoque reactivo, que solo añade pruebas al final.

En cambio, el **SSDLC** mitiga riesgos al integrar análisis de vulnerabilidades, configuraciones inseguras y dependencias de terceros durante el desarrollo.

### Reducción de Vulnerabilidades

Integrar la seguridad en cada fase reduce significativamente las vulnerabilidades críticas desde las etapas iniciales.

### Ahorro de Costes

Ayuda a las empresas a reducir los costos de gestión de brechas de seguridad y mitigación de riesgos.

### Disminución de Incidentes de Seguridad

Las medidas de seguridad proactivas reducen significativamente los incidentes tras el despliegue del software.

### Aumento de la Satisfacción del Cliente

Mejorar la calidad y seguridad del software aumenta la satisfacción de los clientes.

### Mejora de la Eficiencia

Optimiza la eficiencia, reduce los tiempos de desarrollo y mejora la calidad del software.

## ¿Qué *aportamos* en el desarrollo con SSDLC en tu empresa?

La implementación del **SSDLC** en toda la fase del proceso nos ha enseñado que:

### Integración Temprana

Es crucial incorporar la seguridad desde las primeras etapas del desarrollo para garantizar su efectividad.

### Formación Continua

Invertir en la capacitación continua de los desarrolladores es esencial para mantenerlos actualizados en seguridad.

### Automatización de Pruebas

La automatización de pruebas de seguridad, como **SAST**, **SCA** y **DAST**, es clave para identificar y mitigar riesgos de forma eficiente.

### Colaboración Interdepartamental

La cooperación entre los equipos de desarrollo, seguridad y operaciones es fundamental para el éxito del **SSDLC**, naciendo la figura del **DevSecOps.**

## Ventajas de *adoptar* el SSDLC en tu empresa

1. **Evaluación Inicial de Riesgos**
   Realización de un análisis de riesgos de seguridad al inicio del proyecto.
2. **Planificación y Modelado de Amenazas**
   Incorporación de un modelo de seguridad en la planificación e identificación de amenazas para definir los requisitos de seguridad.
3. **Capacitación del Personal**
   Asignación de recursos a la formación continua de desarrolladores y equipos involucrados en el desarrollo.
4. **Uso de Herramientas de Seguridad**
   Implementación de herramientas **SAST**, **SCA** y **DAST** para la detección de vulnerabilidades durante el desarrollo y las pruebas.
5. **Monitorización Continua**
   Establecimiento de monitorización constante y revisiones periódicas para mantener la seguridad del software ante nuevas amenazas.

## Resumen

### Enfoque de seguridad

El **SDLC** se enfoca en entregar software sin priorizar la seguridad, mientras que el **SSDLC** la integra desde el inicio.

### Fases de seguridad

El **SSDLC** incorpora la seguridad en cada fase del desarrollo (Modelado de amenazas, Static Application Security Testing (**SAST**), Software Composition Analysis (**SCA**), Dynamic Application Security Testing (**DAST**), Hardening) mientras que el **SDLC** no.

### Prevención de vulnerabilidades

El **SSDLC** detecta y mitiga vulnerabilidades durante el proceso, no solo tras la finalización del desarrollo.