

TFC CyberSkills 2024 ■

{ Ciberseguridad en el Desarrollo Web }

Estrategias para crear
aplicaciones seguras

- Javier Guerra
- Robin Gómez
- Ryan Salaya

2025-01-30

THE BRIDGE DIGITAL TALENT ACCELERATOR

 **incibe**
INSTITUTO NACIONAL DE CIBERSEGURIDAD

El Equipo

{ Ciberseguridad en
el Desarrollo Web }



Javier Guerra

Técnico Superior DAW
Docente TIC
Programador Full Stack
Administrador TIC



Robin Gómez

Técnico Superior ASIR
Cisco Certified Network Associate
IT technician



Ryan Salaya

Abogado
Cibercrimen - Privacy GDPR
Consultor CyberStrategy
GRC en Startup Digital

Motivación

Profundizar en las estrategias del desarrollo web seguro
y de las herramientas para el análisis y la gestión de riesgos.

Contexto

{ Ciberseguridad en
el Desarrollo Web }

1. Crecimiento y Complejidad del Desarrollo Web:
Velocidad y Escalabilidad.
2. Falta de concienciación de los riesgos:
Seguridad vs. Celeridad.
3. Equipos rotativos y trabajo remoto
4. Automatización y externalización
5. Impacto de la Inteligencia Artificial (IA)
6. Riesgos Emergentes

«La seguridad no es un producto, sino un proceso»

- Bruce Schneider

Criptógrafo y experto en informática

Objetivo

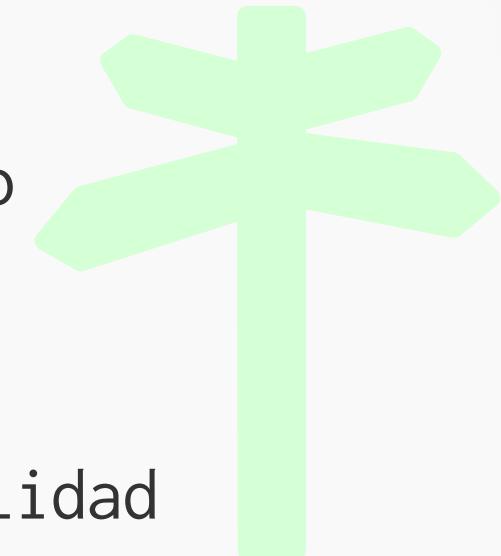
{ Ciberseguridad en
el Desarrollo Web }

Analizar cómo integrar la **ciberseguridad** en el ciclo de vida del **desarrollo de aplicaciones web**, con el fin de fomentar prácticas de desarrollo más seguras, **minimizar riesgos** y garantizar aplicaciones de **mayor calidad** desde las etapas iniciales del diseño.

Riesgos, soluciones, herramientas

{ Ciberseguridad en
el Desarrollo Web }

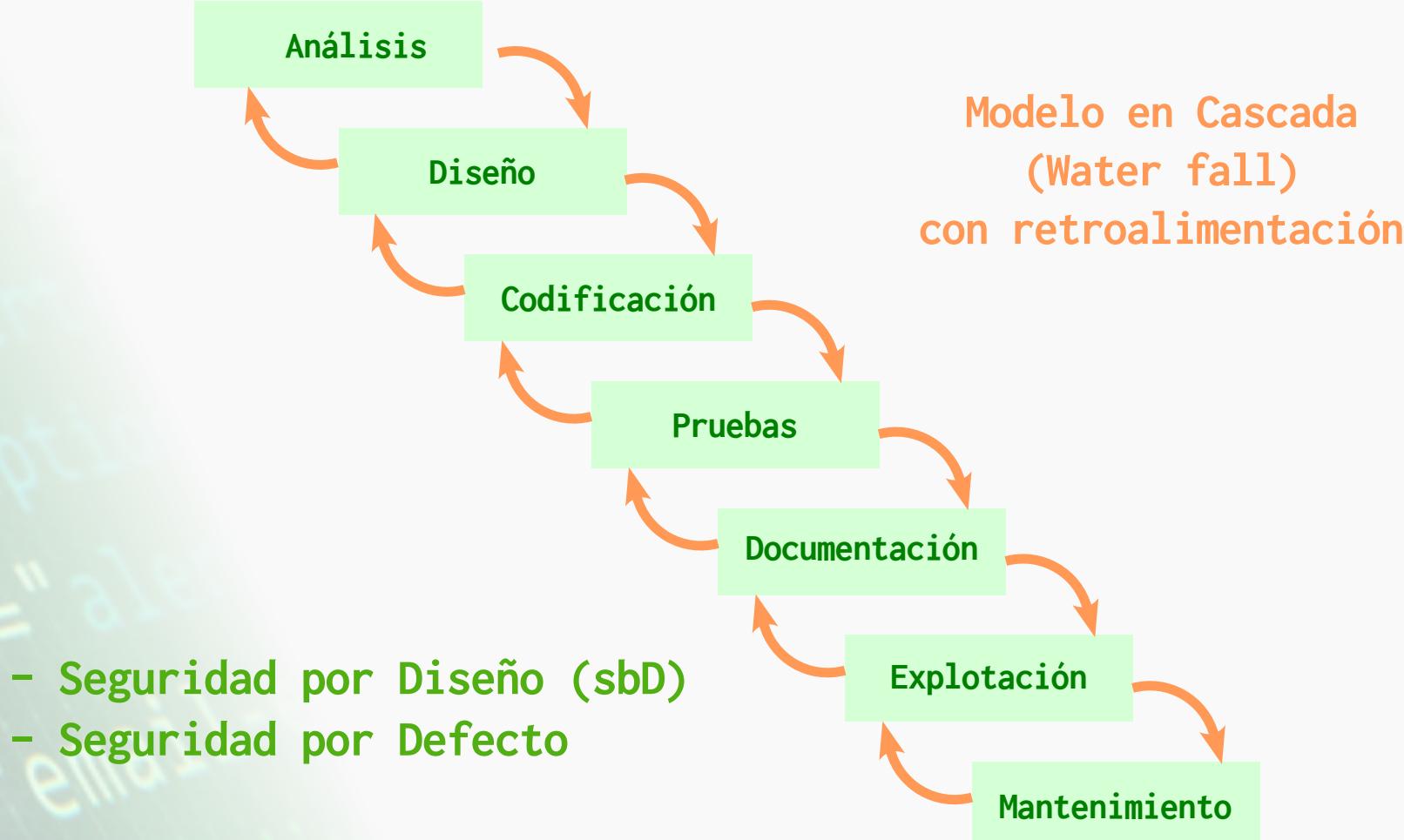
- 0. Nivel de Madurez
- 1. Factor Humano
- 2. Factor Infraestructura
- 3. Bugs de Arquitectura y Diseño
- 4. Bugs de Implementación
- 5. Criticidad del dato
- 6. Test, Validaciones y Trazabilidad



Anexos

Ciclo de Vida

{ Ciberseguridad en el Desarrollo Web }



12 Etapas

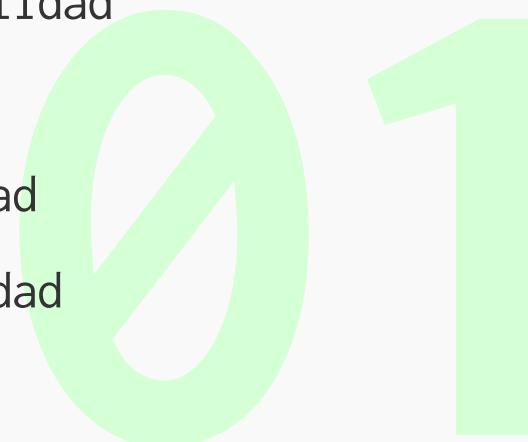
{ Ciberseguridad en
el Desarrollo Web }

01. Planificación, Análisis y Diseño
02. El Desarrollador
03. Trabajo colaborativo
04. Infraestructura para el Desarrollo
05. Herramientas para el Desarrollo
06. Codificación
07. Gestión de los Datos
08. Pruebas
09. Infraestructura para el Despliegue
10. Comunicaciones
11. Monitorización
12. Mantenimiento

Planificación, Análisis y Diseño

{ Ciberseguridad en
el Desarrollo Web }

- No contemplar la seguridad en el diseño
- Desconocer el alcance de los riesgos
- Briefing de requisitos incompleto
- Ausencia de políticas preventivas para la Confidencialidad, Integridad, Disponibilidad
- Metodología de desarrollo inadecuada
- Primar la efectividad vs. la operatividad
- Ausencia de documentos de confidencialidad
- Falta de planificación y de cronología



El Desarrollador

{ Ciberseguridad en
el Desarrollo Web }

- Falta de información sobre el desarrollo
- Falta de formación y concienciación
- Falta de experiencia
- Problemas relacionados con la ingeniería social
- Fugas de información involuntaria (foros, IA...)
- Descuidos en la salvaguarda de información
- Pérdida o robo de equipos
- Desconocimiento del potencial de las herramientas
- Mal uso de las herramientas de desarrollo
- Relajación en los criterios de seguridad a cumplir
- Seguridad insuficiente en el puesto de trabajo

Trabajo colaborativo

{ Ciberseguridad en
el Desarrollo Web }

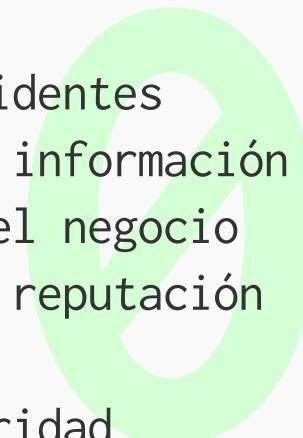
- Uso inadecuado de los recursos compartidos
- Uso compartido de contraseñas
- Recursos compartidos inseguros
- Edición simultánea de documentos
- Distintas versiones de documentos e inconsistencias entre ellos
- Uso de canales de comunicación inseguros
- Criterios y/o planificación deficientes



Infraestructura para el Desarrollo

{ Ciberseguridad en el Desarrollo Web }

- Accesos inseguros y/o desactualizados
- Certificados de acceso no renovados
- Infraestructura mal configurada
- Infraestructura desactualizada o mal parcheada
- Mala gestión o administración deficiente de la infraestructura
- Falta de supervisión, auditoría o trazabilidad
- Ausencia de protocolos de ticketing
- Protocolos y políticas inseguras
- Ausencia de plan de respuesta ante incidentes
- Ausencia de plan de recuperación de la información
- Ausencia de políticas de continuidad del negocio
- Ausencia de políticas de gestión de la reputación
- Falta de auditorías de seguridad
- Poca difusión de las políticas de seguridad



4

Herramientas para el Desarrollo

{ Ciberseguridad en el Desarrollo Web }

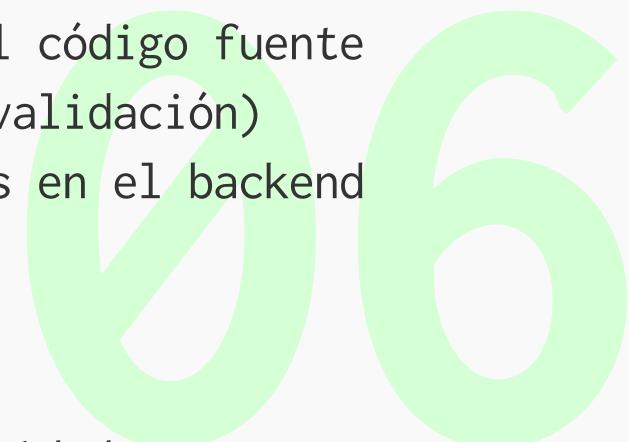
- Versiones de software incompatibles
- Versiones de software inseguro o con dependencias desactualizadas
- Software con acceso no autorizado a información sensible
- Roles insuficientes o roles superiores a los necesarios
- Acceso inseguro a Internet (correo, navegador...)
- Uso de las herramientas inapropiadas
- Shadow IT
- Uso de software de código cerrado



Codificación

{ Ciberseguridad en
el Desarrollo Web }

- Falta de implementación de soluciones para las vulnerabilidades
- Falta de implementación de accesos seguros
- Ausencia de buenas prácticas en el desarrollo
- Uso de lenguajes de programación inseguros
- Ineficiente gestión de la memoria
- Interfaz propensa a errores
- Páginas con datos ocultos (ej. SPA)
- Información sensible distribuida con el código fuente
- Formularios inseguros en el frontend (validación)
- Ausencia de comprobación de formularios en el backend
- Ausencia de controles de edad
- Inyección de código malicioso
- Ausencia de documentación del código
- Uso de políticas de seguridad por oscuridad



- Ausencia de copias de seguridad o copias infrecuentes
- Ausencia de políticas de caducidad (archivo/eliminación)
- Incumplimiento de derechos ARCO y normativas (ej. RGPD)
- Accesos no autorizados a la información
- Vulnerabilidades del SGBD
- Estructuras de datos mal diseñadas
- Ausencia de uso de transacciones
- Datos de salida excesivos
- Información excesiva tras errores



Pruebas

{ Ciberseguridad en
el Desarrollo Web }

- Ausencia de pruebas de código
- Ausencia de pruebas de rendimiento
- Ausencia de pruebas de explotación
- Ausencia de pruebas de regresión
- Pruebas incompletas
- Pruebas mal diseñadas
- Desatender el resultado de las pruebas
- Uso de los datos de producción en las pruebas

Problema:
Coste

08

Infraestructura para el Despliegue

{ Ciberseguridad en el Desarrollo Web }

- Inconsistencias entre las versiones de código de dev y despliegue
- Inconsistencia en las versiones de software entre dev y despliegue
- Ausencia de histórico y versionado de software
- Inconsistencias en el versionado de software
- Ausencia o falta de supervisión de los Pull Request
- Repositorios inseguros
- Ausencia de rollback de los despliegues
- Ficheros de configuración mal implementados
- Incumplimiento de los criterios establecidos para CI/CD
- Servidores compartidos inseguros (VPS, Cloud...)
- Inconsistencias en la virtualización de sistemas
- Inconsistencias en el uso de contenedores
- Inconsistencias en el uso de infraestructuras compartidas
- Ausencias de cachés y otras optimizaciones (balanceo de carga...)
- Sobrecarga de la infraestructura

- Vulnerabilidades explotables en el modelo cliente-servidor
 - Interceptación (escucha o monitorización)
 - Denegación del servicio (interrupción)
 - Modificación (manipulación o alteración)
 - Suplantación (impostura o fabricación)
- Vulnerabilidades P2P
- Ruptura de las estructuras de blockchain
- Uso de protocolos obsoletos y/o inseguros
- Cifrado inseguro
- Uso de hardware inseguro
- Acceso inseguro a APIs y microservicios
- Autenticación y autorización poco robusta
- Acceso inseguro a rutas de la aplicación

1



Monitorización

{ Ciberseguridad en
el Desarrollo Web }

- Ausencia de telemetría y analíticas
- Ausencia de monitorización de anomalías y amenazas
- Ausencia de respuestas automatizadas (ej. limitar intentos login)
- Ausencia de herramientas de administración y supervisión
- Ausencia de sistemas de propuesta de mejoras



- Falta de mantenimiento
- Software desactualizado en línea
- Software de desarrollo desactualizado
- Falta de actualizaciones de dependencias
- Incompatibilidades entre actualizaciones
- Credenciales antiguas
- Ausencia de renovación de pruebas
- Implementación de soluciones temporales

12

1. **Comprensión del riesgo y sus consecuencias:** Reconocer qué las vulnerabilidades son un problema y su impacto en cascada.
2. **Creación de código seguro:**
Ser capaz de escribir y entregar código sin vulnerabilidades.
3. **Sensibilización dentro del equipo:**
Capacidad para educar y enfatizar la importancia de la seguridad.
4. **Definir y liderar estrategias de seguridad:**
Implementar programas de seguridad en el nivel departamental.
5. **Fomentar una cultura de seguridad organizacional:**
Integrar la ciberseguridad en cada nivel.

Soluciones

{ Ciberseguridad en
el Desarrollo Web }

1. Implementar herramientas diseñadas para desarrolladores:

Soluciones integradas en los IDE que faciliten la detección y corrección de vulnerabilidades.

2. Fomentar la educación continua:

Proveer formación práctica y recursos accesibles que mejoren las habilidades de seguridad desde el primer día.

3. Reforzar los procesos existentes:

Mejorar los flujos de trabajo sin imponer cambios drásticos que afecten la productividad.

Fuente: [https://programacion.net/articulo/es-hora-de-un-cambio:
-mejorar-las-habilidades-de-seguridad-en-los-desarrolladores_3408](https://programacion.net/articulo/es-hora-de-un-cambio-mejorar-las-habilidades-de-seguridad-en-los-desarrolladores_3408)

{ Ciberseguridad en el Desarrollo Web }

- Cybersecurity and Infrastructure Security Agency, National Security Agency, Federal Bureau of Investigation, & Australian Cyber Security Centre. (2023). **Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default.** Retrieved from https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf
- Open Web Application Security Project. (2025). OWASP. Retrieved from <https://owasp.org/>

GRACIAS ■

FIN