

{ Ciberseguridad en el Desarrollo Web }

Estrategias para crear
aplicaciones seguras

Javier Guerra



<https://javguerra.github.io/>

2025-01-30

TheBRIDGE DIGITAL
TALENT ACCELERATOR

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

La Web

{ Ciberseguridad en
el Desarrollo Web }

- Interacción en la Web 2.0
- Tu vida está en Internet, dinero, trabajo, amigos...
- Necesitas seguridad en el Mundo paralelo

Web = Apps interconectadas

- La importancia de la prevención
Aplicaciones seguras
- La lógica de tener un plan
Ciclo de vida del desarrollo de aplicaciones

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

- Bruce Schneider
Criptógrafo y experto en informática

Los retos del desarrollo web hoy

1. Crecimiento y Complejidad:
Velocidad y Escalabilidad
2. Falta de concienciación de los riesgos:
Seguridad vs. Celeridad
3. Equipos rotativos y trabajo remoto
4. Automatización y externalización
5. Riesgos Emergentes (p ej. IA)

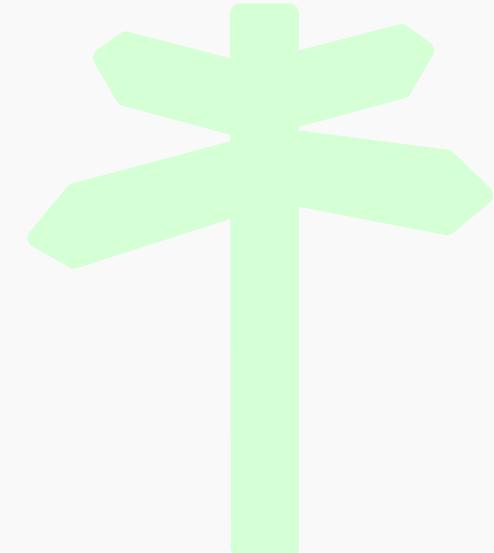
Objetivo

{ Ciberseguridad en
el Desarrollo Web }

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

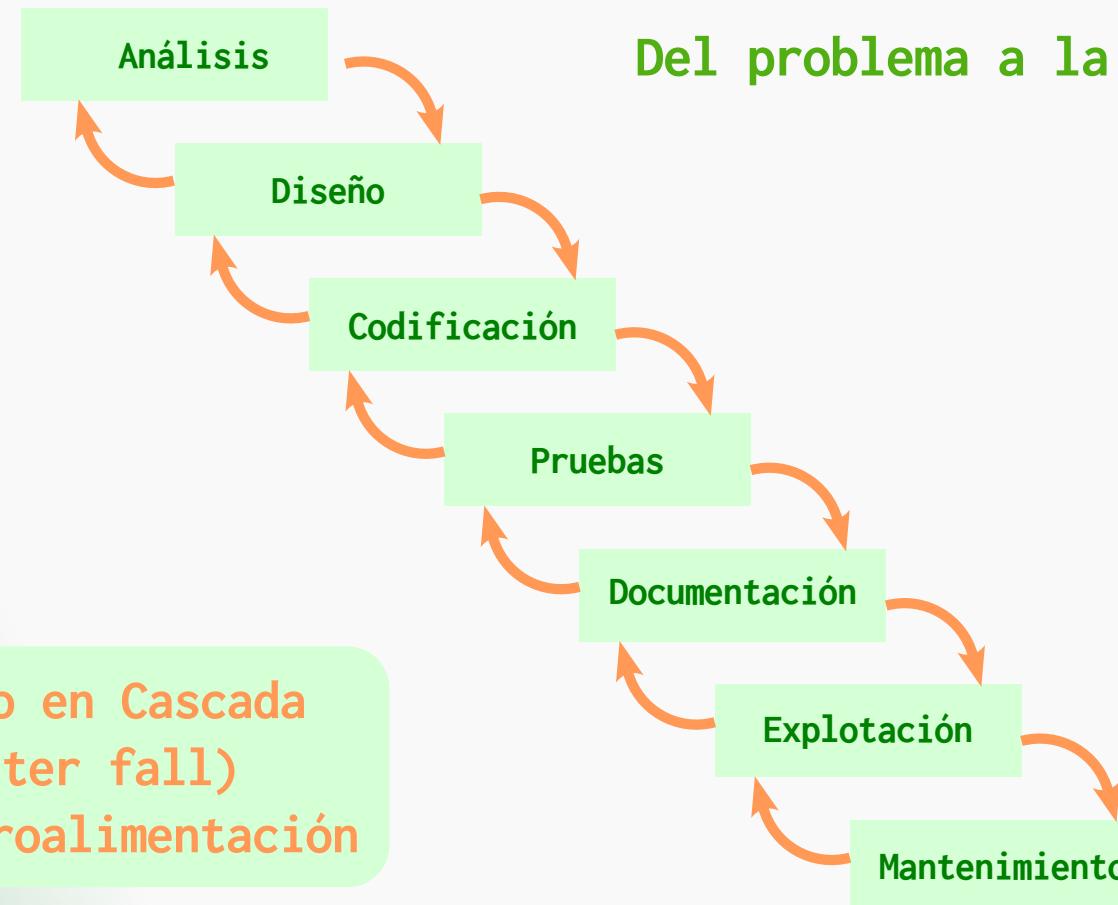
Riesgos generales

1. Nivel de implicación
2. Factor Humano
3. Infraestructura
4. Diseño y desarrollo
5. Criticidad del dato
6. Implantación y seguimiento



Ciclo de Vida

{ Ciberseguridad en el Desarrollo Web }



12 Directrices

{ 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 y documentación
 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 }

- Diseñar una estrategia de seguridad eficiente desde el inicio
 - Adecuada Planificación
 - Prevención para:
 - Reducir riesgos
 - Reducir costes
- Seguridad por Diseño (sbD)
- Seguridad por Defecto



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



Trabaja en equipo, con herramientas e infraestructura y sigue criterios normativos y de conformidad.

Responsabilidades

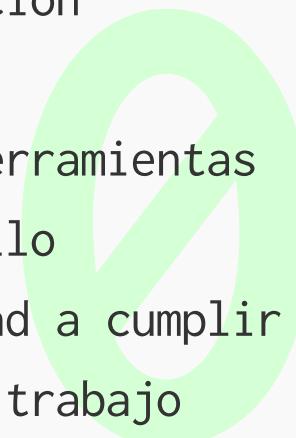
- Concienciación
- Preparación
- Implicación



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



El trabajo se divide en partes

Las partes deben encajar

Responsabilidades

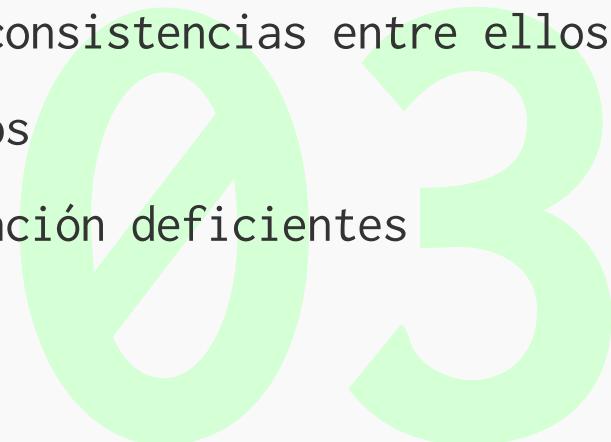
- Planificación
- Coordinación
- Implicación del responsable



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 de colaboración y/o planificación deficientes



Infraestructura para el Desarrollo

{ Ciberseguridad en
el Desarrollo Web }

Determina la forma en que se trabajará
Requiere implicación de varios actores coordinados

Responsabilidades

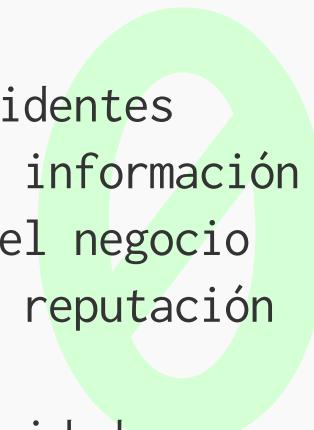
- Planificación de la gerencia
- Prevención
- Revisión continua
- Elaboración de planes de respuesta



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



Herramientas para el Desarrollo

{ Ciberseguridad en el Desarrollo Web }

Software

Materiales de consulta

Depende de la infraestructura

Responsabilidades

- Mantenimiento IT para evitar el Shadow IT
- Uso adecuado de los recursos



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 y Documentación

{ Ciberseguridad en el Desarrollo Web }

Desarrollo + Infraestructura + Herramientas
Directriz determinante del plan

Responsabilidades

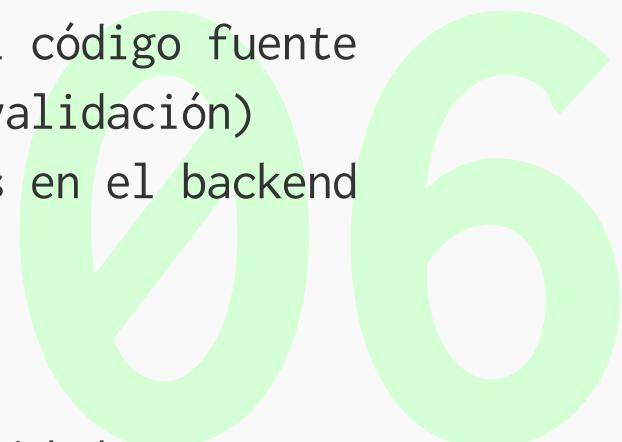
- Evitar sobrecostes



Codificación y Documentación

{ 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



TODO gira en torno a esto: programas usan datos
Complementa la codificación

Responsabilidades

- Priorizar su gestión
- Hacer un uso adecuado de los datos
- Cumplir normativa



- 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 }

Tiempo

Horas / Hombre

Problema:
Coste

Responsabilidades

- Varios tipos de prueba
 - Código
 - Rendimiento
 - Explotación
 - Regresión (tras mantenimiento)

08

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



Infraestructura para el Despliegue

{ Ciberseguridad en el Desarrollo Web }

Repositorios (versionado, ramas...)

Redes

Servidores

Responsabilidades

- Gestión DevOps
- Gestión IT
- Gestión SysAdmin



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 de la red

Accesos inseguros a rutas y servicios

Responsabilidades

- Interceptación (escucha o monitorización)
- Denegación del servicio (interrupción)
- Modificación (manipulación o alteración)
- Suplantación (impostura o fabricación)

10



- Vulnerabilidades explotables en el modelo cliente-servidor
- 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



El software está vivo en la red:

nace > crece > se reproduce > interacciona > muere

Responsabilidades

- Supervisión
- Reportes



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

El software se desactualiza:

Funcionalidades

Dependencias

Responsabilidades

- Planificar de nuevo

12

- 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 }

Material de consulta básico

- 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