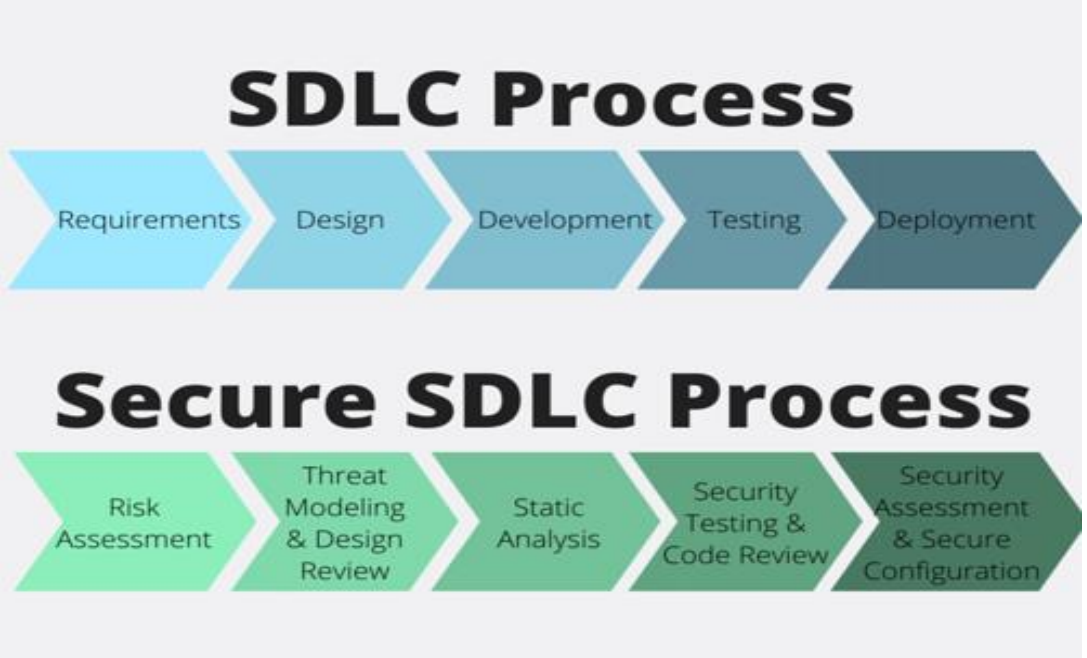
Seguridad de la Información & Ciberseguridad

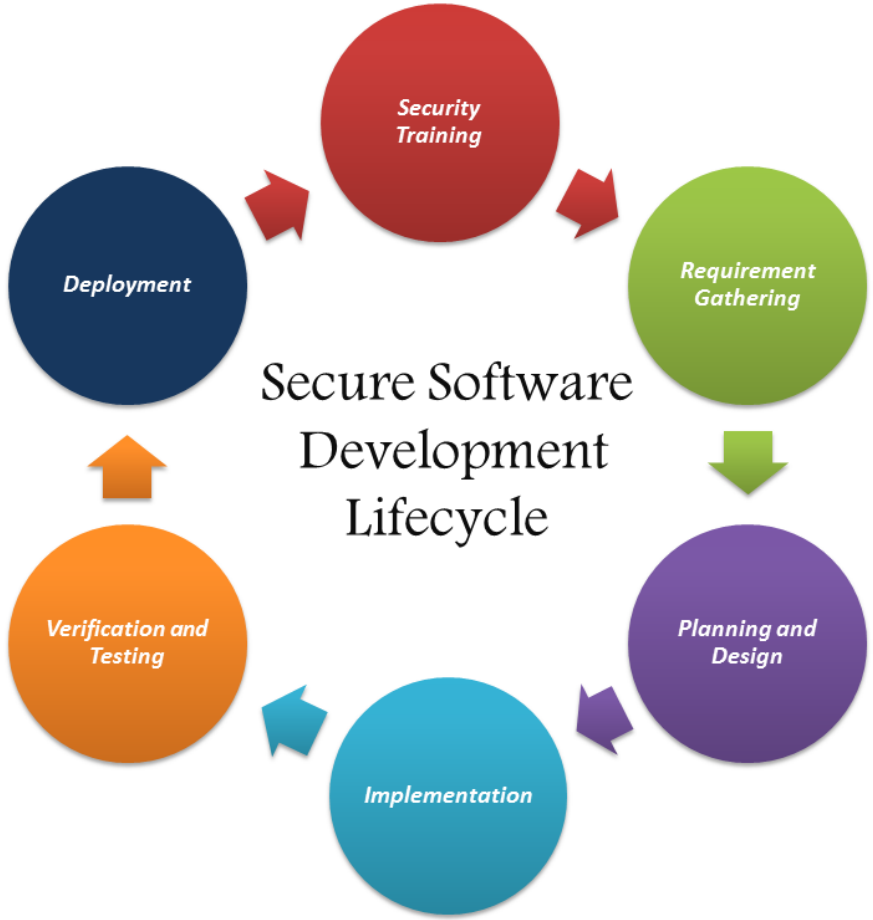
La ventaja de incorporar prácticas de ciberseguridad en el ciclo de vida de desarrollo de software

Agosto 2022

PROSA ACADEMIA

Ciclo de Vida de Desarrollo Seguro de Software





PROSA ACADEMIA

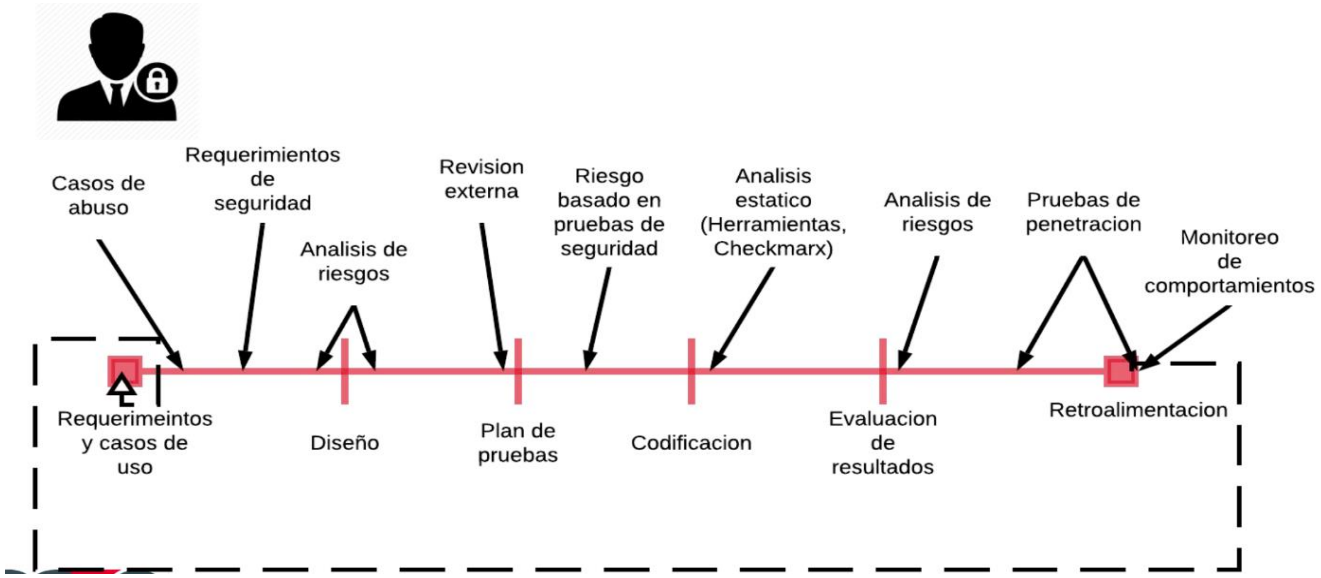
Seguridad en el Ciclo de Vida de Desarrollo Seguro de Software

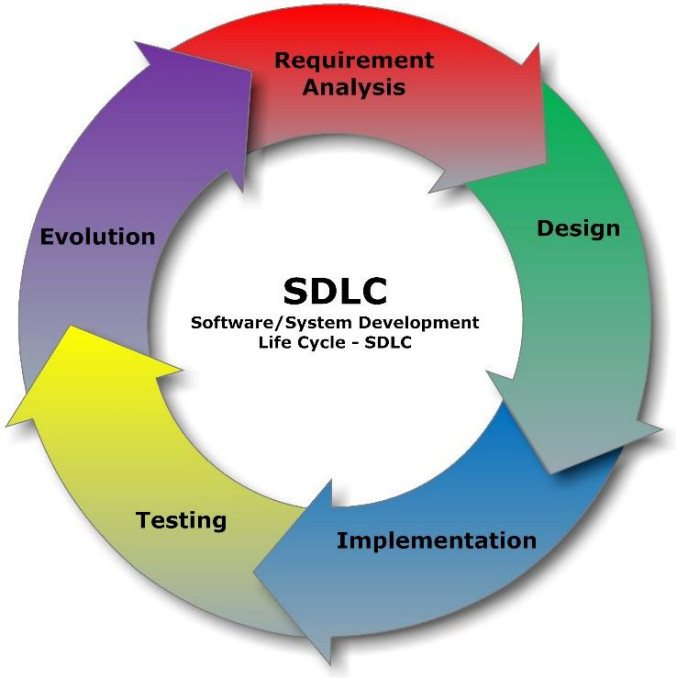
¿Que es?

SDLC son las siglas de: Systems Development Life Cycle, también conocido como "System Design Life Cycle" (ciclo vital del desarrollo/diseño de sistemas).

"Software Development Life Cycle" sinónimo de proceso de desarrollo de software.

Agregando elementos de seguridad al ciclo de desarrollo de Software podemos tener:
sSDLC = Security on System Development Lifecycle.



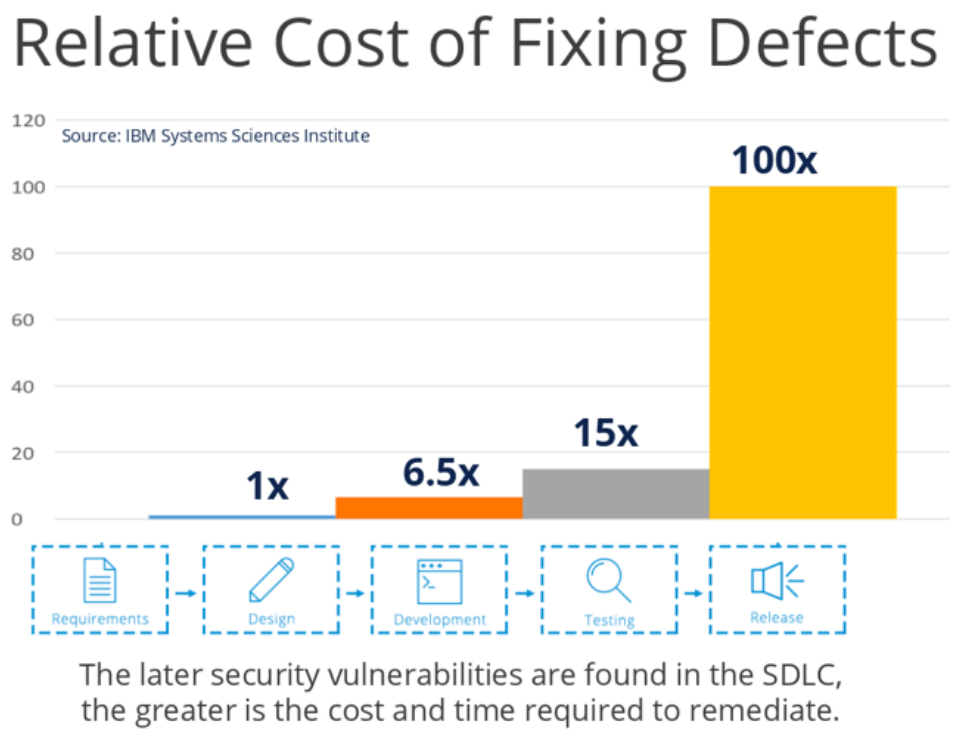


Fuente: (ISC)2 Certified Information Systems Security Professional Official Study Guide, Seventh Edition, James Muchael Stewart, Mike Chapple, Darril Gibson 2015.

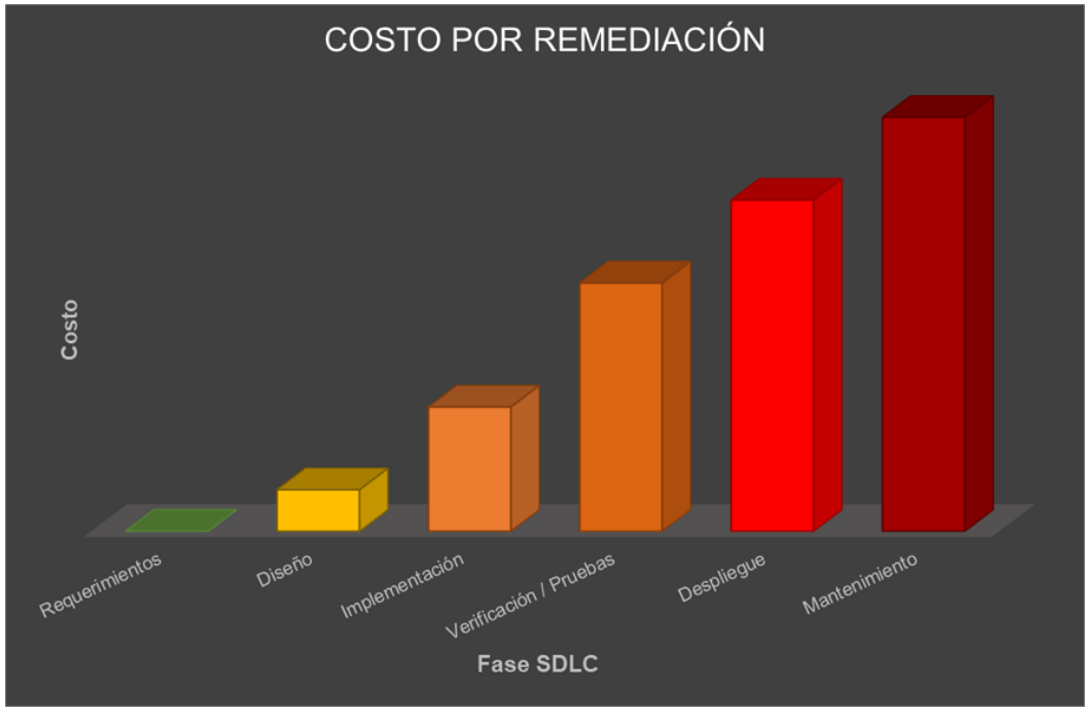
PROSA ACADEMIA

Seguridad en el Ciclo de Vida de Desarrollo Seguro de Software

IBM demuestra que es 100 veces más costoso reparar un defecto después de su lanzamiento, que durante la fase de diseño.



Fuente: https://blog.securitycompass.com/how-to-sell-training-costs-internally-756b1c731f0a



Fuente: https://www.magazcitum.com.mx/index.php/archivos/5490#.Yg6wat_MI2w

PROSA ACADEMIA

Los equipos con documentación de calidad son

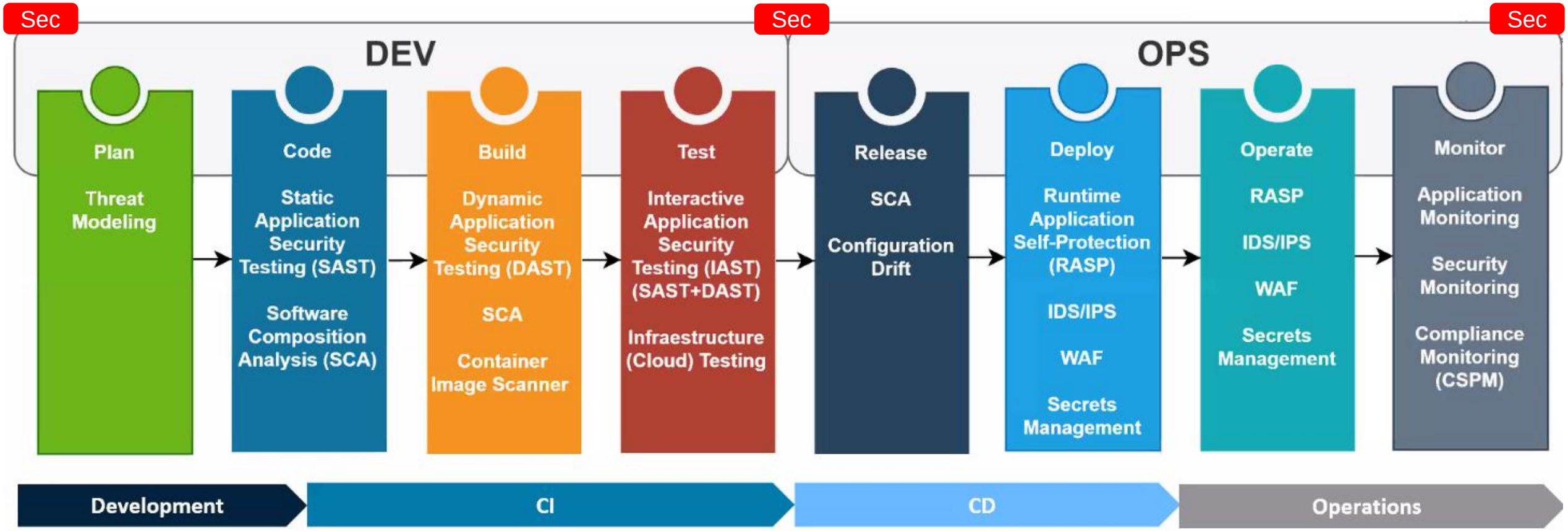
3.8x

más propensos a implementar prácticas de seguridad

Cultura

Fuente: Informe Accelerate del State of DevOps 2021 by Google

DEV OPS



PROSA ACADEMIA

Fases del Ciclo de Vida de Desarrollo Seguro de Software

1. Entrenamiento	2. Requerimientos	3. Diseño	4. Implementación	5. Verificación	6. Liberación	7. Respuesta
1. Capacitación de Seguridad aplicada al ciclo de desarrollo	2. Establecer los requerimientos de Seguridad, aplicables al proyecto.	5. Establecer los requerimientos y/o recomendaciones con perspectiva de Seguridad.	8. Usa herramientas autorizadas para el desarrollo de software.	11. Ejecutar un análisis de vulnerabilidades dinámico.	14. Ligar este desarrollo a nuestro proceso de gestión de incidentes de Seguridad.	Ejecutar un proceso de respuesta a Incidentes conforme al plan de Seguridad contra ataques Cibernéticos.
	3. Crear puertas de calidad / barras de errores.	6. Evaluar la superficie de ataque y activos de la información involucrados.	9. Eliminar el uso de funciones depreciadas y/o consideradas obsoletas o inseguras.	12. Realizar remediación de Vulnerabilidades.	15. Realizar validaciones finales desde la perspectiva de Ciberseguridad (Pentest).	
	4. Realizar un análisis de riesgos desde la perspectiva de Seguridad y Privacidad.	7. Usar un modelado contra amenazas informáticas y seguir Frameworks de Seguridad.	10. Ejecutar un análisis de vulnerabilidades estático.	13. Evaluar el nivel de cumplimiento vs la regulación aplicable al sistema.	16. Certificar desde Seguridad de la Información que se atendieron los requisitos y/o recomendaciones.	

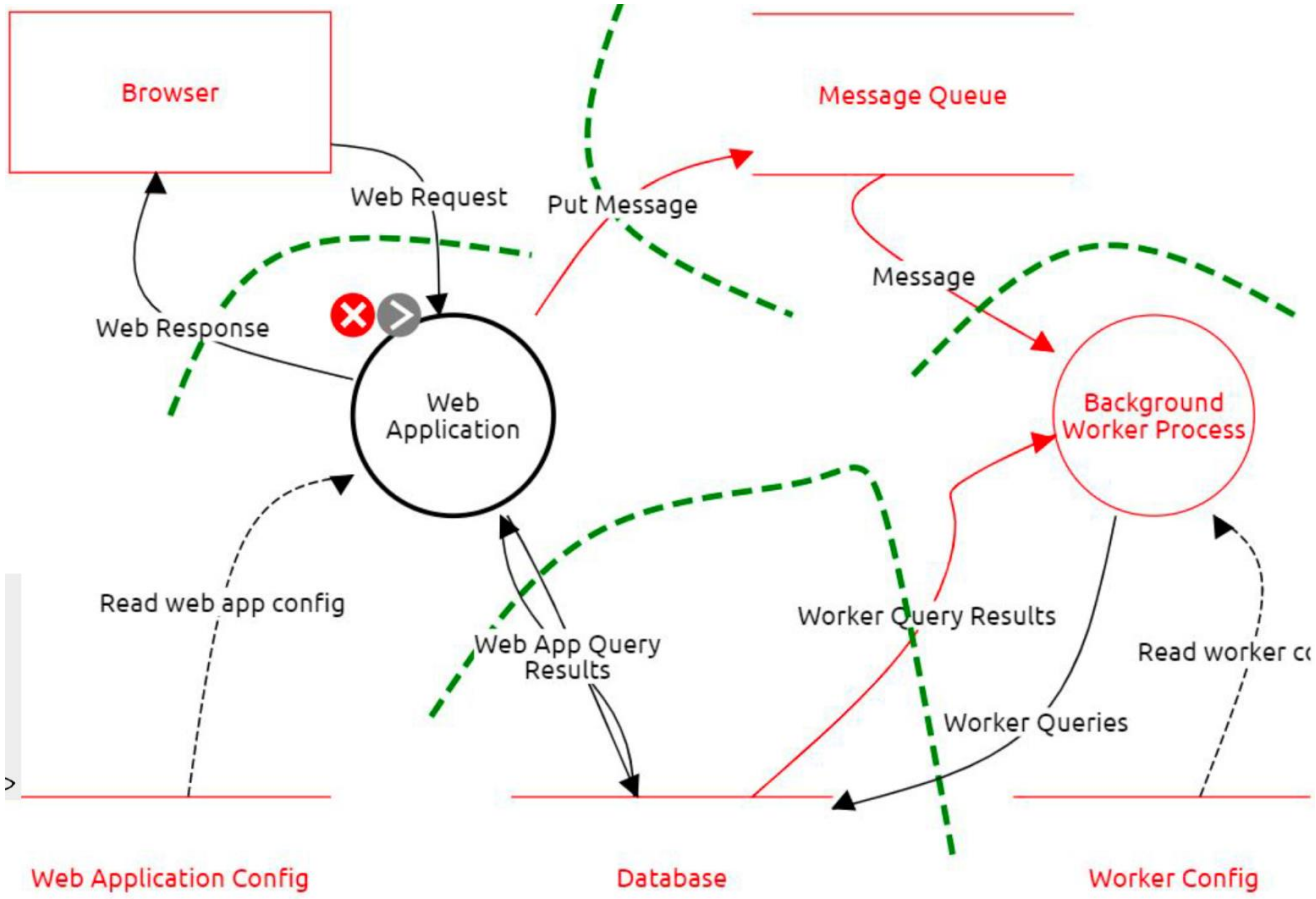
ISO 27000-Series

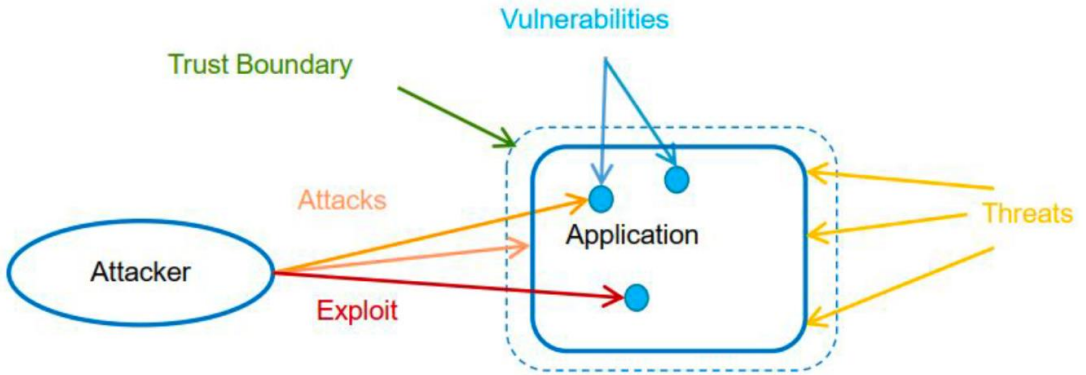
8. Mejora Continua

PROSA ACADEMIA

Fuente: (ISC)2 Certified Information Systems Security Professional Official Study Guide, 8th Edition.

Modelado de amenazas



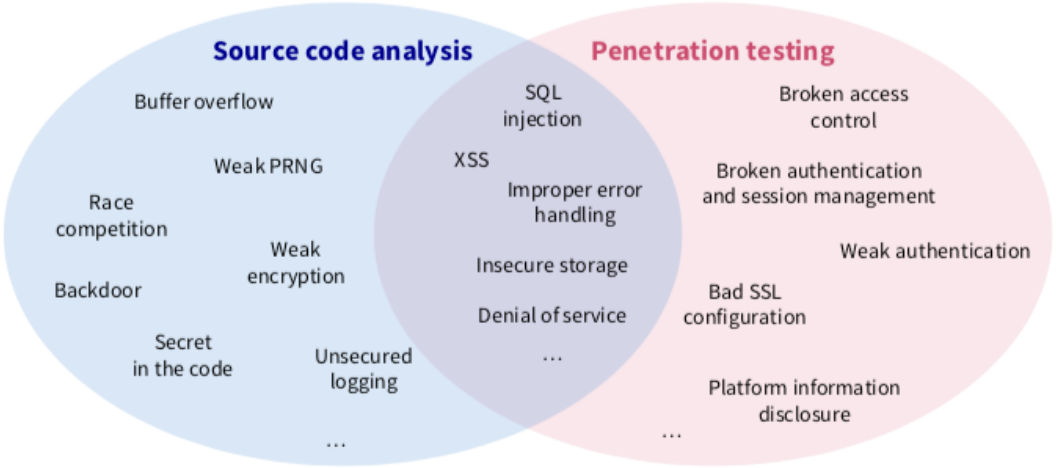


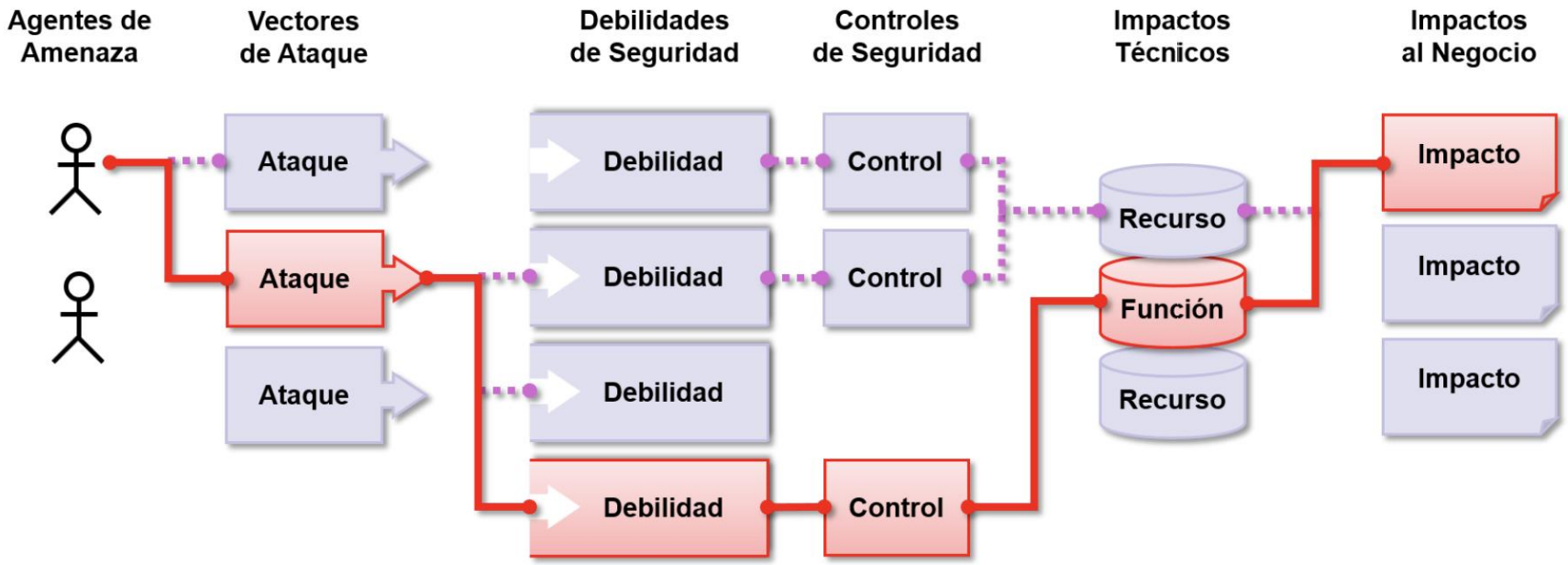
Mandatory Security Activities	GAP
Security Classification	!
Security Requirement Specification	!
Dynamic Review	✓
Source Code Review (only Critical and High)	!
Security Requirement Validation	!
Pentest Campaign	✓
Basic tests	✓

Fuente: (ISC)2 Certified Information Systems Security Professional Official Study Guide, 8th Edition.

PROSA ACADEMIA

Agentes de amenaza y cómo prevenirlos

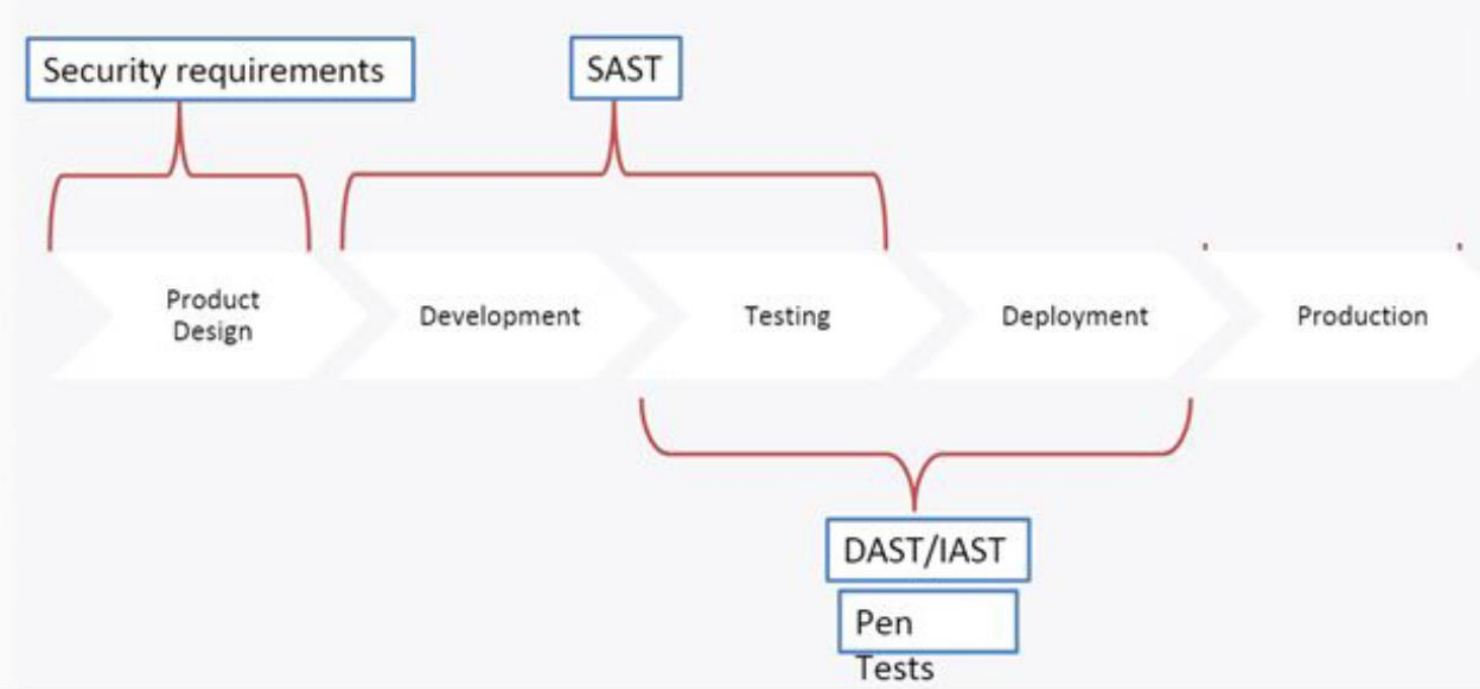




PROSA ACADEMIA

Herramientas de revisión de código

- SAST – Static Application Security Testing
- DAST – Dynamic Application Security Testing
- IAST – Interactive Application Security Testing



PROSA ACADEMIA

Estándares de Seguridad para el Desarrollo Seguro

The 2021 OWASP Top 10 list

A01:2021 Broken Access Control	**A02:2021** Cryptographic Failures	**A03:2021** Injection	**A04:2021** Insecure Design	**A05:2021** Security Misconfiguration
A06:2021 Vulnerable and Outdated Components	**A07:2021** Identification and Authentication Failures	**A08:2021** Software and Data Integrity Failures	**A09:2021** Security Logging and Monitoring Failures	**A10:2021** Server-Side Request Forgery

Microsoft® Security

OpenSAMM

OWASP Open Web Application Security Project

ORACLE

BSIMM

SAFECode Software Assurance Forum for Excellence in Code Driving Security and Integrity

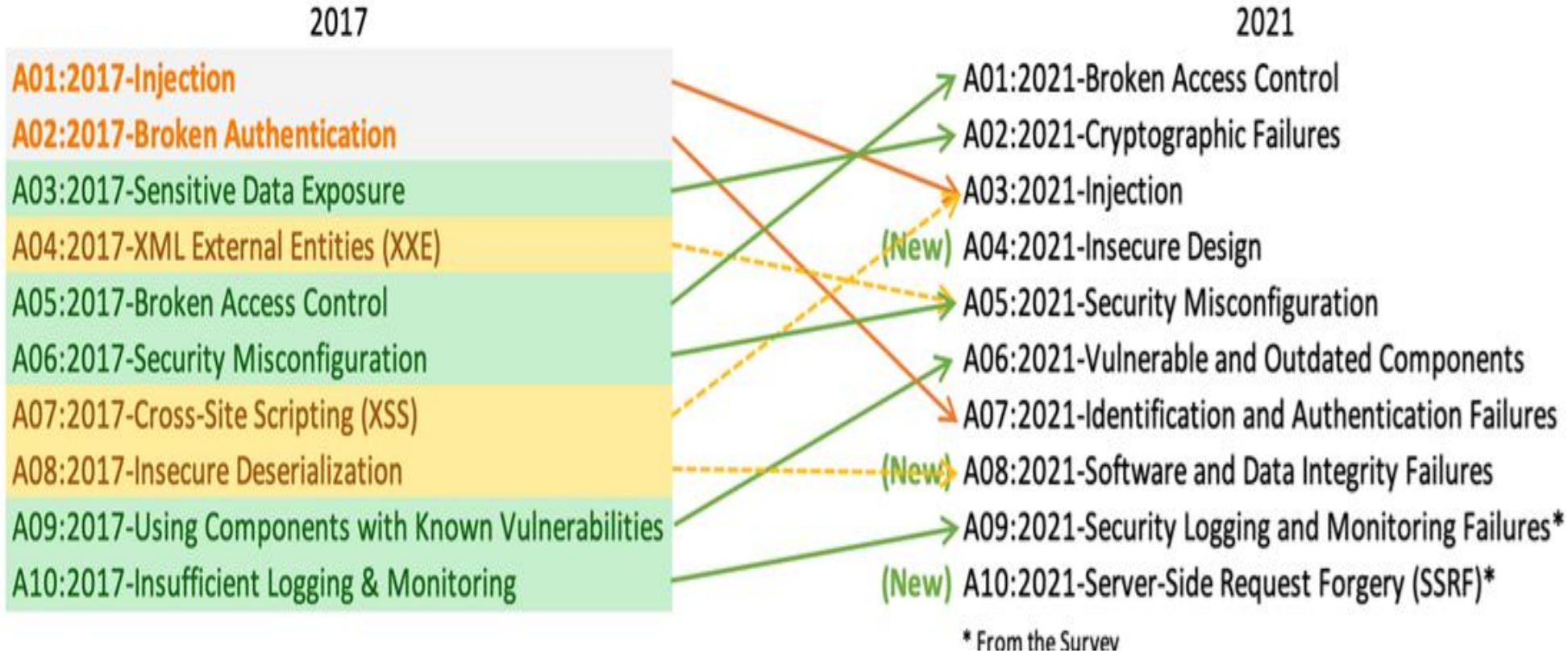
Software Engineering Institute Carnegie Mellon

Fuente: https://owasp.org/Top10/

PROSA ACADEMIA

Estándares de Seguridad para el Desarrollo Seguro

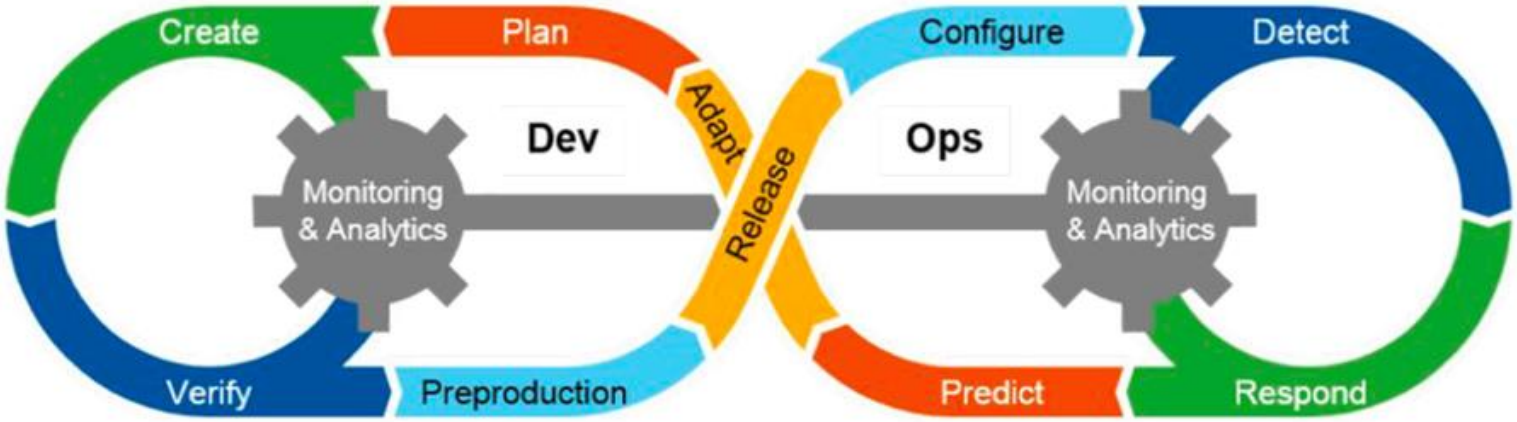
OWASP
Open Web Application Security Project



Fuente: https://owasp.org/Top10/

PROSA ACADEMIA

[Shift-left] e integración completa



Fuentes:
https://cwe.mitre.org/data/definitions/699.html
Codecov hack — likened to SolarWinds — targets software supply chain | Cybersecurity Dive

Práctica de seguridad	
Prueba la seguridad	58%
Integra la revisión de seguridad en cada fase	54%
Revisa la seguridad	60%
Crea código preaprobado	49%
Integra la revisión de seguridad en cada fase	63%

Fuente: Informe Accelerate del State of DevOps 2021 by Google

PROSA ACADEMIA

GRACIAS

PROSA ACADEMIA