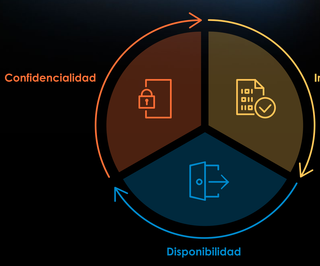
Desarrollo seguro

CCN centro criptológico nacional

Desde el origen de la Seguridad de la Información hasta la actualidad el principal **vector de ataque** son las **aplicaciones**.

TRIADA CIA

La ciberseguridad se basa en **tres pilares básicos** que protegen la privacidad de los datos y el secreto de la información, mantiene inalterada la información ante accidentes o intentos maliciosos y garantizan el acceso a la información conforme el propósito de negocio y durante el periodo temporal requerido.



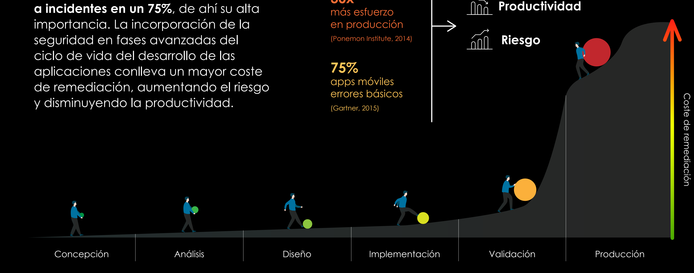
S-SDLC

Las organizaciones que aplican la metodología S-SDLC (*Secure Systems Development Life Cycle*) ven **reducidos sus costes de gestión** de la configuración **y de respuesta a incidentes en un 75%**, de ahí su alta importancia. La incorporación de la seguridad en fases avanzadas del ciclo de vida del desarrollo de las aplicaciones conlleva un mayor coste de remediación, aumentando el riesgo y disminuyendo la productividad.

84% brechas en cada aplicación (Gartner, 2013)

30x más esfuerzo en producción (Ponemon Institute, 2014)

75% apps móviles errores básicos (Gartner, 2015)

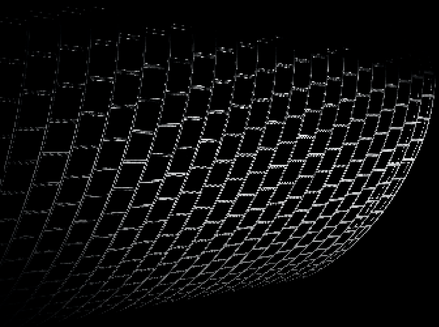


MODELADO DE AMENAZAS

Técnica de ingeniería que **identifica posibles amenazas y recomendaciones** para ayudar a reducir el riesgo y cumplir los objetivos de seguridad en estadios anteriores del ciclo de vida de desarrollo.

Diseño — **Interrupción** — **Corrección** — **Verificación**

DIRECTRICES DE CODIFICACIÓN SEGURA



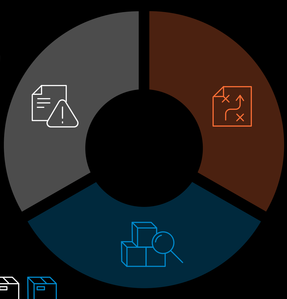
- Seguridad en las transacciones
- Seguridad en las comunicaciones
- Control de acceso. Autorización
- Gestión segura de archivos
- Arquitectura
- Autenticación
- Gestión de la sesión
- Validación de la entrada
- Codificación de la salida
- Tratamiento de errores
- Registro
- Criptografía
- Protección de datos

TÉCNICAS DE ANÁLISIS

En la fase de validación del SDLC, se realizan una serie de test, entre ellos se encuentran los test de seguridad de código (SAST), de terceros (SCA) y de comportamiento (DAST):

SAST
(Static Application Security Testing)

Análisis de caja blanca. Proporcionan un análisis de seguridad del código fuente, lo que permite detectar los puntos débiles y las posibles vulnerabilidades en las primeras fases del desarrollo.



DAST
(Dynamic Application Security Testing)

Análisis del comportamiento de la aplicación, probando cómo responde a ataques especialmente diseñados. Permite definir con mayor precisión el impacto de vulnerabilidades dentro de la aplicación.

SCA
(Software Composition Analysis)

Permite conocer qué librerías de código abierto están en uso y ser conscientes de las vulnerabilidades que pueden contener y afectar a la seguridad de toda la aplicación.

CCN-CERT centro criptológico nacional