

# Análisis estático de código

---

# Análisis estático de código

---

Es el proceso de evaluar el código **sin ejecutarlo**

- Para:
  - Facilitar el desarrollo y el mantenimiento
  - Evitar costos posteriores por código mal elaborado

# Generalidades

---

- Busca encontrar defectos en:
  - Código fuente
  - Modelos de software
- Se realiza **antes** de las pruebas dinámicas
- Por lo general usa herramientas automáticas (aunque puede ser manual)

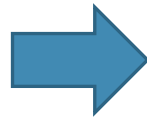
```

int totalNewFeatures = 3;
int totalWorkingNewFeatures = 0;
float numberOfBugs = 345889E+08;
boolean readyForRelease = FALSE;

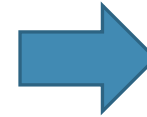
void main {
    while (!CRASHED) {
        if (first_time_install) {
            if ((installedRAM < 2GB) ||
                (processorSpeed < 4GHz))
            {
                MessageBox("Hardware incompatibility error.");
                GetKeyPress();
                BSOD();
            }
        }
        Make10GBswapfile();
        SearchAndDestroy(FIREFOX|OPENOFFICEORG|ANYTHING_GOOGLE);
        AddRandomDriver();
        MessageBox("Driver incompatibility error.");
        GetKeyPress();
        BSOD();
    }
}

```

Código fuente



Analizador



Sugerencias y advertencias

# El análisis estático encuentra:

---

- Violaciones a principios de diseño
- Violaciones a estándares de programación (incluyendo comentarios)
- Vulnerabilidades de seguridad
- Código que se puede optimizar
- ...

# Ventajas

---

- Encuentra defectos que no son fáciles de identificar en las pruebas
- Se identifica la causa (facilita corrección)
- Ejecución barata
- Ayuda a prevenir defectos

# Limitaciones

---

- No permite analizar la funcionalidad ni que el software sea correcto
- Puede cambiar con cada lenguaje de programación (sobre todo estándares)
- Falsos positivos / Falsos negativos

# ¿Cuándo realizar análisis estático del código?

---

- De acuerdo al riesgo
- Posibilidades:
  - Con nuevas funcionalidades o correcciones
  - Periódicamente (integrar en el proceso de desarrollo)



# Repaso

---

- ¿Para que se realiza el análisis estático de código?
- ¿Qué tipos de problemas encuentra el análisis estático de código?
- ¿Qué limitaciones tiene este tipo de análisis?