Fallas y vulnerabilidades

DigitalHouse >
Coding School

Certified Tech Developer
The Ultimate Degree

Índice

1 | Fallas

“

Una **falla**, también conocida como bug, es un **error** en un programa o sistema operativo que desencadena un resultado indeseado.

”

“El término **bug** viene desde 1947 cuando Grace Hopper, mientras estaba programando el Mark II, descubrió que un **insecto** (bug) había provocado un error en uno de sus relés electromagnéticos.”

“En el desarrollo del software existen muchos tipos de fallas, pero en general se pudieron establecer unos tipos generales de bugs según su comportamiento.”

Tipos de fallas

Nombre	Descripción
Heisenbug	Basados en el principio de incertidumbre de Heisenberg se denominan a aquellos bugs que alteran o desaparecen su comportamiento al tratar de depurarlos.
Bohrbug	Nombrados así por el modelo atómico de Bohr, es una clasificación de un error de software inusual que siempre produce una falla al reiniciar la operación que causó la falla.
Mandelbug	Llamado así por el matemático Benoit Mandelbrot, un mandelbug es un fallo con causas tan complejas que su comportamiento es totalmente caótico.
Schroedinbugs	Son errores que no aparecen hasta que alguien lee el código y descubre que, en determinadas circunstancias, el programa podría fallar. A partir de ese momento, el "Schroedinbug" comienza aparecer una y otra vez.

2 | Vulnerabilidades

Una **vulnerabilidad** es una debilidad o fallo de un sistema informático que puede poner en riesgo la integridad, confidencialidad o disponibilidad de la información.

“

La evaluación o detección de vulnerabilidades permite reconocer, clasificar y caracterizar los agujeros de seguridad.

”

Pasos para detectar una vulnerabilidad

Si bien no existe un método único para detectar vulnerabilidades, es posible armar una serie de ítems a tener en cuenta para considerar nuestra información segura.

- Evaluar cómo está constituida la red e infraestructura de la empresa.
- Delimitar quién puede y debe acceder a la información confidencial.
- Probar que las copias de seguridad realizadas funcionen.
- Identificar las partes más sensibles y esenciales del sistema.
- Realizar auditorías del estado de la seguridad informática.


DigitalHouse>
Coding School