TÉCNICO EN
SEGURIDAD INFORMÁTICA

Nivel 4

NIVELES DE SEGURIDAD INFORMÁTICA

Capacítate para el empleo | FUNDACIÓN Carlos Slim

El estándar más usado a nivel internacional para definir los niveles de seguridad informática está desarrollado por el Departamento de Defensa de los Estados Unidos en el TCSEC (Criterios Confiables para la Evaluación de Sistemas Computacionales por sus siglas en inglés), mejor conocido por Orange Book (libro naranja).

En él se definen las medidas de seguridad que debe seguir una red de equipos informáticos y las clasifica en 4 niveles de seguridad:

Nivel

D Protección mínima

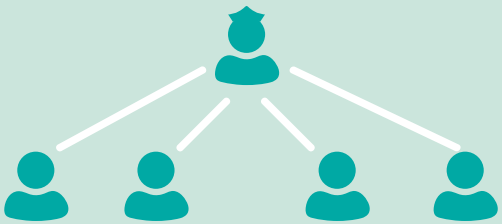
Aquí se encuentran los sistemas informáticos que no son seguros, ya que no cuentan con mecanismos para restringir el acceso al sistema.

C Protección discrecional

Los sistemas de este nivel son aquellos en los que cada usuario tiene acceso a diferente información. Por ejemplo, un equipo o red que cuenta con un "Administrador" y varias cuentas de "Usuario".
Existen dos subclases en este nivel:

C1 **Protección de seguridad discrecional:** La base de datos del sistema permite que cada usuario tenga acceso a su información y la protege de otros que podrían leerla, alterarla o borrarla.

C2 **Protección de acceso controlado:** El administrador implementa procedimientos de acceso seguro y puede monitorear las acciones de los usuarios del sistema.



NIVELES DE SEGURIDAD INFORMÁTICA

Nivel

B Protección obligatoria

Son sistemas que utilizan reglas de control de acceso. La información almacenada tiene un grado de sensibilidad definido (secreto, privado, etc.), para saber quiénes pueden acceder a ella.

- **B1** **Seguridad etiquetada:** Cumple con los requisitos del subnivel C2. Además debe ser capaz de etiquetar con precisión la información que se envíe. En este subnivel, el control de acceso es obligatorio. Algunos usuarios tienen un permiso para acceder y modificar datos específicos.
- **B2** **Seguridad estructurada:** En estos subsistemas, el modelo de políticas de seguridad debe estar expresado en un documento formal. Este nivel de seguridad requiere que todos los usuarios tengan permisos específicos para acceder a los datos que contiene el sistema.
- **B3** **Dominios de seguridad:** Los subsistemas con este nivel, todas las medidas de seguridad, tanto físicas (como cortafuego por hardware) como lógicas (por ejemplo, software de control de acceso) deben probarse para comprobar que son casi invulnerables ante amenazas de seguridad.

A Protección verificada

Este nivel requiere que todos los controles de seguridad del sistema se prueben, para asegurar que mantienen segura toda la información almacenada y procesada.