# Softline Penetration Test

Ayudamos a las organizaciones a minimizar los riesgos y reducir sus vulnerabilidades por medio de assessments de seguridad con foco en la educación y concientización de los usuarios.

Un Penetration Test es una técnica utilizada para evaluar la seguridad de los recursos y activos de una organización.

Un consultor especializado en la materia, realiza la prueba con el objetivo de identificar las vulnerabilidades existentes en la infraestructura y analizar el entorno completo en profundidad. Se busca no solo identificar las vulnerabilidades, sino también ponerlas a prueba para entender el impacto en la organización, donde fallan los controles y las brechas que pueden existir entre la información crítica y las políticas existentes.

El Penetration Test puede ejecutarse desde un punto de vista interno o externo. En el interno, se tiene acceso a recursos y datos de la organización sobre los cuales se buscan las vulnerabilidades. En el externo el análisis se enfoca en las aplicaciones o servicios expuestos en internet, es decir aquellos que son más propensos a ser atacados.

## Objetivos del PenTest:

- Conocer en detalle el estado de la seguridad del entorno evaluado (organización, sistema, etc) en ese momento.
- Analizar cuán vulnerable es su organización a la vista de hackers.
- Comprender el impacto real de las vulnerabilidades, brechas y falta de controles en el entorno evaluado.
- Validar la correlación entre las políticas existentes y las vulnerabilidades identificadas.
- Evaluar la efectividad de la Estrategia de Seguridad actual de la organización (políticas, accesos, manejos de información, etc).

## Las etapas asociadas a este servicio son:

- Reconocimiento
- Análisis e identificación de vulnerabilidades
- Explotación de vulnerabilidades y brechas
- Realización, entrega y análisis de reportes

## ¿Por qué debería realizar un PenTest?

Las amenazas y estilos de hackeos se van perfeccionando, es por ello que las organizaciones deben contemplar la evaluación de la seguridad de sus sistemas. En base a los resultados se conoce cual es el estado de situación, y se puede elaborar un plan de ajuste y revisión periódica

## Reportes

Luego del PenTest, se elaboran 2informes donde se explica y acompaña a la organización en la corrección de fallas y el establecimiento de nuevas políticas y procesos.

- **Informe ejecutivo:** describe el nivel de riesgo de la compañía en general, mostrando las problemáticas por medio de conceptos claros y gráficas.
- **Informe técnico:** tiene como objetivo acompañar al área de TI en la resolución de falas y vulnerabilidades encontradas. Se muestran las evidencias de los test ejecutados de manera tal que todas las tareas sean repetibles y transparentes para el cliente.