Advance security testing Red Team

Scope

The Red Team exercises are simulated tests from the point of view of a real attacker, whose scope is to evaluate different areas of action (Digital) in order to create realistic attack vectors, to test the protection of the Entity against a targeted attack and thus determine the weaknesses and failures in the security and cybersecurity controls established and implemented.

The scope of the project is to simulate a real and controlled intrusion in the technological infrastructure of Banco de Occidente through different approaches in an identical way as an attacker would do it.

Advance security testing Red Team

Target

Perform a simulation of real and controlled attacks with the aim of taking control of the organization, trying to access assets with critical and confidential corporate information. For this purpose, a series of intrusion tests combining different attack vectors within the digital environment will be used. This allows to identify the level of exposure and risk faced by the organization, and thus, its overall security level, as well as the level of prevention and protection against targeted threats.

Different scenarios and attack vectors that can be identified and exploited are addressed, some of which include:

- Digital Intrusion
- Social Engineering
- Physical Intrusion.