EVOTING SECURITY

In the digital world there are multiple situations that could eventually jeopardize the effectiveness of the services we provide. That is why we have paid special attention to those elements to prevent them and, in case they occur, to neutralize them.

Our IT security measures are grouped into **6** areas:

- **Academic support:** we base all our development on public algorithms from Academia, which have therefore been tested, approved and are recognized.
- **Technical team:** top IT professionals who monitor processes in real time and in constant communication with our EVoting Operations team. They prevent malicious scenarios and quickly mitigate any anomaly.
- **Monitoring:** installation of multiple servers in different geographical areas, with real-time monitoring systems and different alarms, depending on the number of voters per second and number of visits to the different servers. In case of any problem, backup systems are automatically activated.
- **IP monitoring:** to avoid possible irregularities, we limit the number of votes accepted per IP, depending on the election.
- **Anti-hacking protection measures:** the entire platform is hosted on Amazon Web Services, which has the highest standard in security and protection, and allows us to control where the data is stored, who can access it and what resources are consumed at any given time.
- **Ethical hacking:** EVoting undergoes an annual ethical hacking test by expert security teams. The last test was conducted between March and April 2021, with the final report delivered in July, certifying that the vulnerabilities are fully mitigated.