

Cláusulas de ciberseguridad



GRUPO POPULAR



Infrastructure As A Service

1. **Logical access control.** **THE PROVIDER**, in compliance with the requirements for security control for access to systems or Software, must guarantee the following:
 - a. Protect the confidentiality of all passwords or access codes assigned to **THE SUPPLIER**.
 - b. Have a password policy under which its personnel, including employees, subcontractors and/or service suppliers, manage password changes every ninety (90) days or more frequently, avoiding trivial or obvious passwords in accordance with the best security standards.
 - c. timely withdraw the privileges of logical access to the personnel of **THE PROVIDER**, including employees, subcontractors and/or service suppliers who, either by internal transfer or termination of the relationship with **THE PROVIDER**, or if applicable, the corresponding subcontractors, cease to be involved, for whatever reason, in the processing of information and data of **BANCO POPULAR**.

2. **Infrastructure security.** To ensure the integrity, confidentiality, and availability of all the information and data of Grupo Popular and its subsidiaries, and to mitigate the threat, risk and impact of improper use and external or internal abuse thereof, **THE PROVIDER** must apply the following information security requirements:
 - a. install, configure, and activate a comprehensive intrusion protection system (network and host), in accordance with industry best practices, so that it continuously prevents, detects, and reports the occurrence of unauthorized network attacks and against your systems, including, without limitation, penetration attempts, denial-of-service attacks and excessive polling, etc.
 - b. install industry best practice network firewalls between servers and gateways to the public network to exclude communication protocols not needed to process Internet traffic.
 - c. Protect the information of **BANCO POPULAR** against unauthorized disclosure during its transit through public networks, or its authorized personnel, its clients, or subcontractors, guaranteeing the security of the data owned by **BANCO POPULAR**, using encryption techniques based on best practices. accepted in the industry.
 - d. Protect access to all equipment, of any nature, including communications equipment, servers, perimeter equipment, at a minimum, through a combination of user identification (ID) and secret password without this implying a limitation to implement additional access and authentication security measures.
 - e. Change passwords at least every ninety (90) days or more frequently.
 - f. Ensure that their teams are located in physically safe areas and have alternate sites in cases of natural disasters, cases of force majeure, or induced.



- g. Reinforce the security of all the equipment that is used to process, store or transmit data and information of **BANCO POPULAR**, by virtue of the execution of this contract, such reinforcement must include, among others, the elimination of all access and service privileges except those that are essential for the execution of the operations for which said servers are installed.
- h. Implement security analysis tools or description of the process used to periodically report the status of each piece of equipment and verify that all configurations, parameters, and options are in accordance with the agreed hardening status for that device and to detect unauthorized changes and updates necessary from the baseline of the approved configuration.
- i. Identify vulnerabilities and threats, and implement a continuous investigation process with reliable sources for these that may impact the operating environments or platforms used by **THE PROVIDER** for the processing of **BANCO POPULAR** data,
- j. Record all activity on the infrastructure (Communications equipment, Servers, Perimeter equipment) or audit logs, in an appropriate manner for a continuous period and online according to industry best practices or for an online retention period according as requested by Grupo Popular.
- k. **BANCO POPULAR** reserves the right to carry out penetration tests on the services offered by **THE PROVIDER**.

PARAGRAPH I: To ensure compliance with the requirements of information security of **BANCO POPULAR**, current legal regulations on the matter, and industry best practices for data backup and recovery, **THE PROVIDER** must:

- a. Implement appropriate backup measures, including storage of backup data files in secure locations off the processing site, to enable efficient system recovery;
- b. Facilitate the resumption of critical applications and business activities in a timely manner after an emergency or disaster.
- c. Maintain a documented disaster recovery and/or contingency plan for each critical system related to **BANCO POPULAR** and for business applications and test it annually.

PARAGRAPH II: **BANCO POPULAR** reserves the right to carry out periodic reviews related to compliance with the controls agreed in this contract. If any finding is identified in any of the infrastructures of **THE PROVIDER**, it will be reported to them, and **THE PROVIDER** must commit to correct it according to best industry practices.

- 3. **Compliance.** **THE PROVIDER** guarantees that the systems, licenses, or subscriptions for solutions that are being contracted and that handle Personally Identifiable and Transactional Information will process it in accordance with this agreement, including, but not limited to, privacy or data protection, to all prohibitions of misuse and unfair and deceptive practices, and applicable policies, rules and laws, such as the Payment Card Industry Data (PCI DSS) and Security Standards.



4. **Data security incidents and other breaches.** **THE PROVIDER** will notify **BANCO POPULAR** immediately in the event of a breach of its obligations, in the event that data protection is affected, or any other Data Security Incident, but in no case more than 24 hours after **THE PROVIDER** knows or reasonably suspect such an event. At **THE PROVIDER**'s expense, **THE PROVIDER** will assist and cooperate with **BANCO POPULAR** regarding disclosures to affected parties, the government or regulatory bodies, and other corrective measures as reasonably requested by **BANCO POPULAR** or as required by any applicable law or regulation. applicable privacy or data protection, such cooperation will always include the following:
- a. **THE PROVIDER** will promptly investigate said Data Security Incident and will take all reasonable and necessary measures to identify and mitigate its effects, and with the prior written agreement of **BANCO POPULAR**, to carry out any recovery or other action necessary to remedy the Security of the Data. Data;
 - b. **THE PROVIDER** must expeditiously provide **BANCO POPULAR** with all available information and reports, whether draft or finalized, regarding the incident and must prepare a summary based on **THE PROVIDER**'s full knowledge of the potential impact of the Data Security Incident and the response to actions taken or planned by **THE PROVIDER**.
 - c. As soon as reasonably possible, **THE PROVIDER** will provide **BANCO POPULAR** with a list of names of the natural persons potentially affected, and any other known contact information.
 - d. At the request of **BANCO POPULAR** and at the expense of **THE PROVIDER**, **THE PROVIDER** must adequately notify and remedy the persons whose Personally Identifiable Information has or could reasonably have been affected by the Data Security Incident.
 - e. **THE PROVIDER** may not disclose the existence of the Data Security Incident or any related information without the prior written approval of **BANCO POPULAR**, except when necessary to inform insurers, external legal team advisors and public relations related to **BANCO POPULAR**, in that sense is going to be required to follow the applicable law or regulations, in which case you must provide **BANCO POPULAR** reasonable prior notice were permitted by law to do.