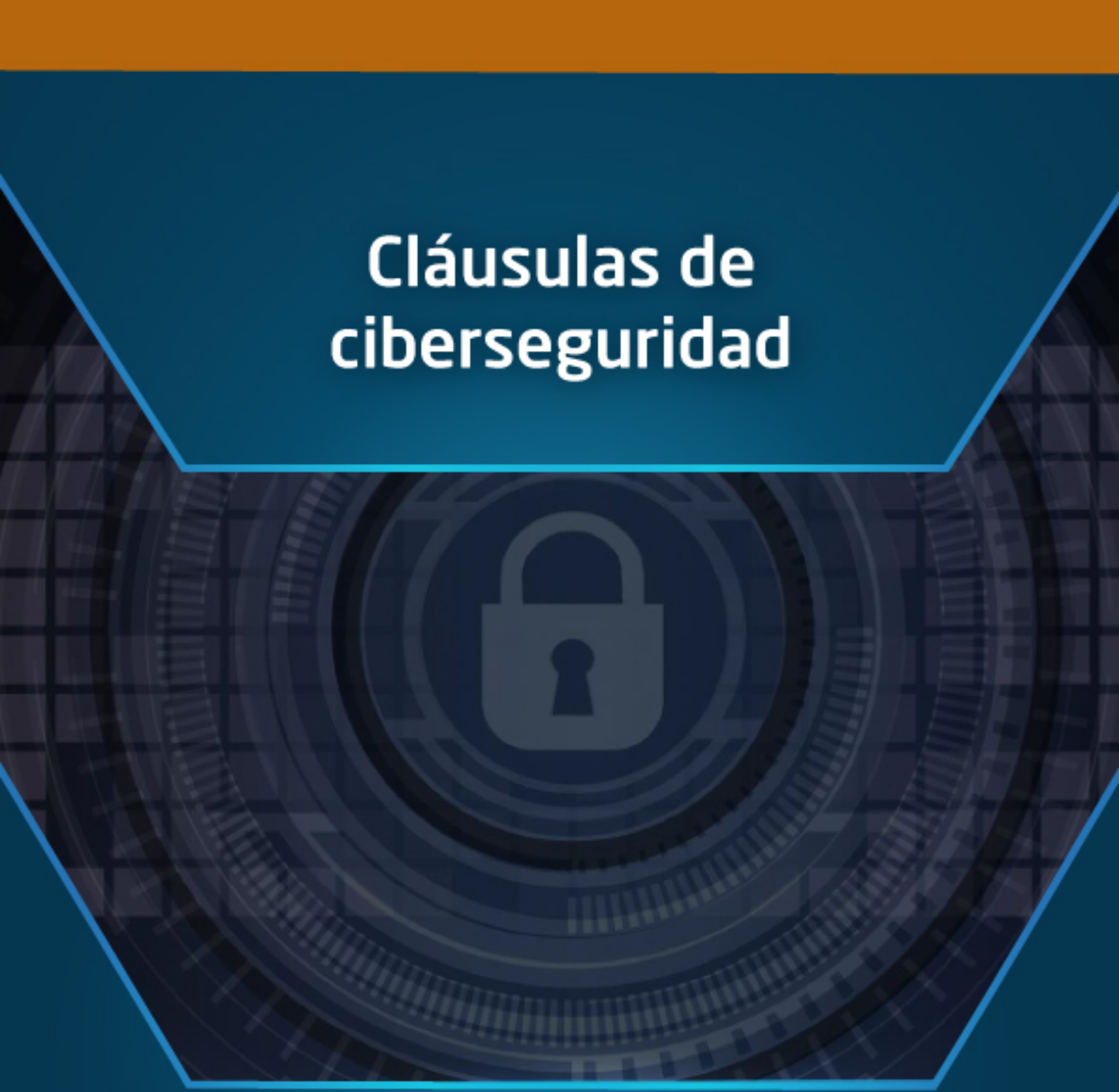
Cláusulas de ciberseguridad



GRUPO POPULAR

Acquisition of Services and Applications to be Installed OnPremises

1. **Viruses, other malicious programs, and information security measures**. **THE PROVIDER** states that the systems, licenses, or subscriptions of solutions that are the object of this agreement, are enabled to protect the Confidential Information and the Personally Identifiable and/or Transactional Information, in accordance with the law and/or applicable commercial regulations. **THE PROVIDER** declares that its performance of the Services and the Services themselves will not introduce viruses or other harmful elements designed to interrupt the orderly operation or damage the integrity of the data files residing in any of the **BANCO POPULAR** equipment. **THE PROVIDER** will make all possible efforts to guarantee that, from the date each Deliverable is sent to **BANCO POPULAR**, said Deliverable does not contain any virus or other harmful element. Consequently, **THE PROVIDER** must, with respect to the systems, licenses, or subscriptions object of this agreement, carry out the following security measures:

   a. Delete any computer code designed to damage, interrupt, disable or prevent in any way the orderly operation of any software, data file, firmware, hardware, computer system or network ("Viruses").
   b. Ensure with reasonable efforts, during the writing, execution and copying of any Software delivered in connection with the Agreement, that such Software is free of any Viruses, prior to delivery, of any Software and any media on which it is to be delivered with a current version of a leading anti-malware application.
   c. The Software will not contain any computer code or any other procedure, routine or mechanism designed to: (a) interrupt, disable, or impair in any way the orderly operation of the Software based on the course of a period of time, exceeding a number authorization of copies, or advance to a particular date or any other measure (sometimes referred to as "time bombs", "time locks" or "defuse devices"); (b) cause the Software to damage or corrupt any of the data, storage media, programs, equipment or communications of any of the Bank's Affiliates, or the data of their respective customers, or to interfere with the operations of the Bank or its Affiliates, or (c) allow **EL SUPPLIER**, its Personnel, its licensors or any other third party, track or monitor the use of, or otherwise access, the Software or Bank Systems for any reason (sometimes referred to as "cheats") access codes "or devices" trap door").
   b. **THE PROVIDER** You must ensure that the software acquired is developed under the best practices of secure development methodologies.
   c. Carry out pretesting and static and dynamic code review whenever a system update is carried out before being delivered to Grupo Popular, to guarantee good safe development practices.

2. **Damage Mitigation.** In addition to, and not instead of, **THE PROVIDER**'s indemnity obligations, if any Service or Deliverable becomes, or is likely to become, the subject of a third-party claim, then **THE PROVIDER** shall: (i) acquire the right of **BANCO POPULAR** and the Indemnified to continue using the Services or Deliverables as contemplated hereinafter; (ii) modify the Services or Deliverables

and make them non-infringing (provided that such modification does not materially degrade the performance, function or operation of the Services or Deliverables); or (iii) replace the Services or Deliverables with equally suitable, functionally equivalent, compatible, and non-infringing Services or Deliverables. If, despite the efforts of **THE PROVIDER** in accordance with the foregoing,

3. **Notification of Third-Party Claims**. **THE PROVIDER** shall immediately notify **BANCO POPULAR** of any threat, warning, claim or action against **THE PROVIDER** or its clients or suppliers, which could have an adverse impact on the use of **BANCO POPULAR** of the Services or Deliverables provided or made available to **BANCO POPULAR** in accordance with this Agreement.

4. **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.

5. **Obsolescence. THE PROVIDER** guarantees that the systems, licenses, or subscriptions for solutions covered by this agreement are duly updated to the latest supported versions available on the market. **THE PROVIDER** must assure **BANCO POPULAR** that the product or solution will be supported by new updates and patching of tools that support its execution.

6. **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 communication to affected parties, the government or regulatory bodies, and other corrective measures as reasonably requested by **BANCO POPULAR** or as required by any law or regulation. of 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, provided that the incident affects the contracted service;
   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** must cooperate with **BANCO POPULAR** to identify the individuals 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, provided that the negligence or breach of the agreement by **THE PROVIDER** with respect to its obligations.
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.

The **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.