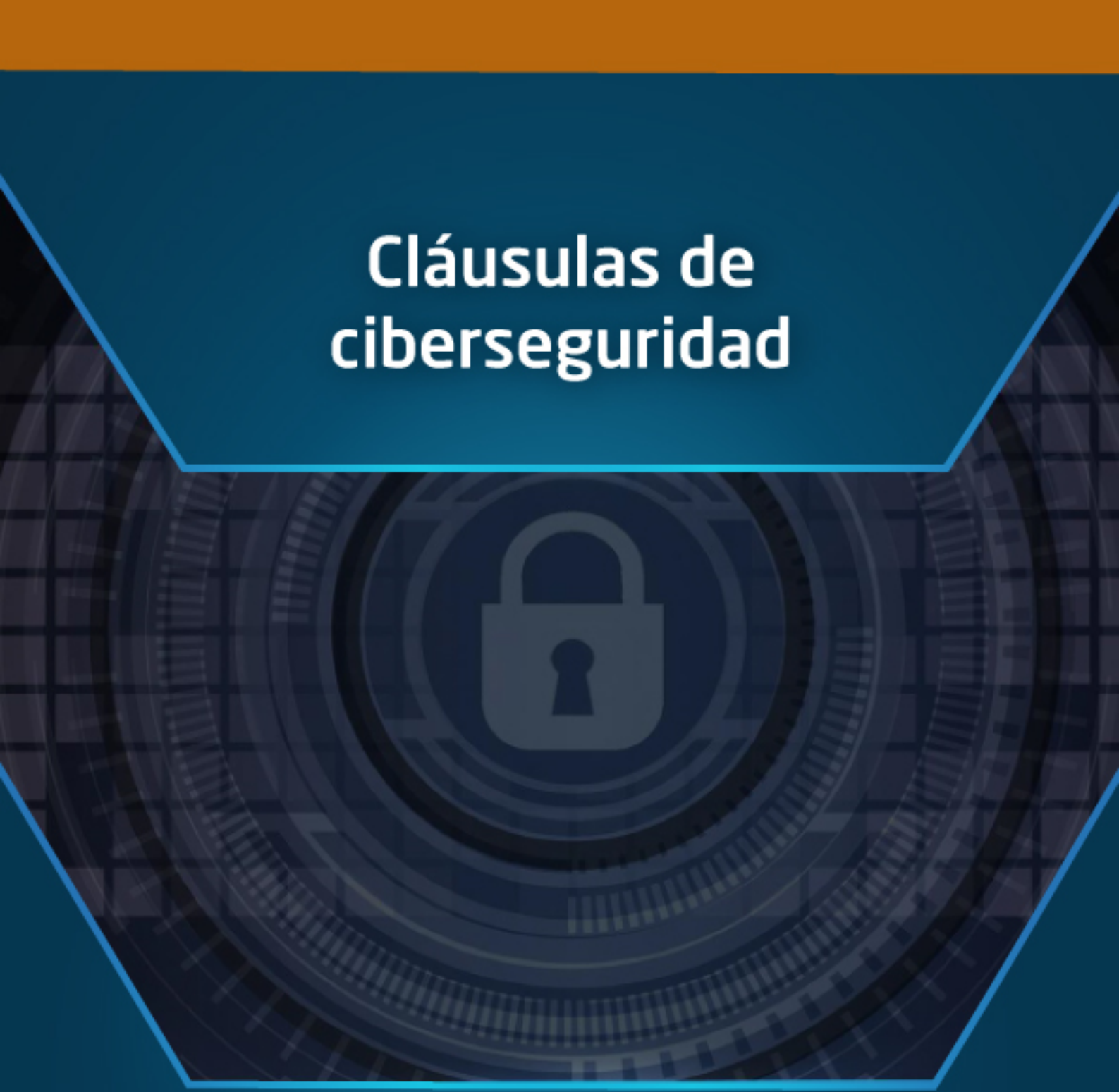
Cláusulas de ciberseguridad



GRUPO POPULAR

Professional Services

1. **Cybersecurity. – THE PARTIES** state that the negotiations carried out (or the project to be developed jointly) between the owner of the information described below, hereinafter the Discloser, and the recipient thereof, hereinafter the Recipient, have involved or will involve written disclosure or verbal and communication to the Recipient by the Discloser or by members of his work team, of documents owned or controlled by any of the aforementioned, which may include, but is not limited to financial information, business plans, personal information, drawings, examples and prototypes of artifacts, demonstrations, trade secrets, technical information, computer systems and software, research results, customer lists and other information in oral or written form related to technology, whether said communication occurs verbally, visually, or through demonstrations or any other means, whether in the form of drawings, models, printed documents, and/or electronic file format or in any other way, hereinafter the Information".

PARAGRAPH I: Confidential Information, and all rights thereto that have been or will be disclosed to the Recipient, shall remain the property of the Discloser. The Recipient will not obtain any right, of any kind, over the information, nor any right to use it, except for the purpose of this agreement. Disclosure of Confidential Information does not imply the license of any patent or copyright right or any other rights on the part of the Discloser, other than those set forth herein.

PARAGRAPH II: THE PROVIDER must have an anti-malware system with anti-exploitation prevention capacity based on the best practices in the industry, in all the equipment that processes or stores confidential or sensitive information and/or any other data of **BANCO POPULAR**, keeping this system updated for the proper protection of the documents and data provided by Grupo Popular.

PARAGRAPH III: THE PROVIDER must have a Third-Party Management policy that contemplates the guidelines for compliance with the services that it needs to subcontract as part of the service that Grupo Popular is requiring and that complies with those set forth in this contract.

PARAGRAPH IV: In the same way, **THE PROVIDER** must maintain an update management and patching of systems in which information belonging to Grupo Popular will be managed, for the prevention of information leakage it must have a system or policies and procedures, or any other DLP mechanism (Data Loss Prevention), according to best industry practices to mitigate this type of risk of information leakage through removable storage devices, USB, Hard Drives, CD, DVD, Email, etc.

PARAGRAPH V: BANCO POPULAR reserves the right to realize periodical revisions related to the compliance of the agreed upon controls in the present contract. Should any findings be identified in any of **THE PROVIDER**'s infrastructures, it will be reported to them, and THE PROVIDER must commit to fix it according to the best industry practices.

PARAGRAPH VI: If **THE PROVIDER** needs at any time to connect to the BANCO POPULAR systems due to the type of service contracted, this must be done through a secure connection and must be configured together with Grupo Popular personnel. Likewise, if information considered confidential and/or sensitive is shared, it must be through secure channels and/or connections, which will be provided by BANCO POPULAR.

PARAGRAPH VII: THE PROVIDER must make proper use of the connections provided by BANCO POPULAR, complying with a series of security guidelines on all devices that connect to our corporate network (and while this connection is active), including, but not limited to: not executing (or preferably not having installed) any type of Instant Messaging, Remote Access, Peer to peer (P2P) or Storage application, and not browsing websites in the categories of Social Networks, Streaming, Downloads, Games, Pornography or Hacking; limiting themselves to making use of the tools authorized by BANCO POPULAR. Any violation of these guidelines will be grounds for blocking the user and initiation of a security investigation.

PARAGRAPH VIII: THE PROVIDER acknowledges and agrees to comply with the following obligations and responsibilities with respect to the personnel that will be providing the service:

a. **THE PROVIDER** undertakes to keep its personnel uniformed and carrying work cards when required, at the time of carrying out the work that is the object of this contract.

b. **THE PROVIDER** undertakes to provide **BANCO POPULAR** with the names and identification cards of the personnel that will be assigned to the service, providing them with identification cards that must be used in a visible manner while they are performing the Services set forth in this Framework Agreement or each of the Service Orders.

c. **THE PROVIDER** undertakes and obliges to carry out the purification of the place to the personnel to be used in the provision of the service object of this contract.

d. **THE PROVIDER** must notify **BANCO POPULAR**, within 24 hours after it occurs, of the departure and dismissal of its personnel who, by virtue of their functions, have the credentials, cards and/or authorizations to access the facilities of **BANCO POPULAR**, so that the latter can take the corresponding control and security measures.