4.1 Protection of Banrep Corporate Information (both physical and electronic)

Corporate information is a strategic asset of Banrep[38] and according to the rules set out below, Banrep employees have a duty to prevent the improper subtraction, destruction, concealment, or use; and they should not allow unauthorized persons to access it.

Numeral 5 of Article 62 of Law 1952 of 2019[39] establishes as gross negligence caused by public servants to produce damage to State computer equipment as well as to alter, falsify, introduce, erase, hide or disappear information from any of the official information systems contained in or stored in them, or to allow access to it to unauthorized persons. Similarly, numeral 18 of Article 39 of Law 1952 of 2019[40] states that public servants could not give access or display files or documents to unauthorized persons.

Numeral 6 of Article 38 of Law 1952 of 2019[41] states that it is the duty of all public servants to custody and protect the documents and information that, due to their job or function, they may have or to which they have access, and prevent improper subtraction, destruction, concealment, or use of it.

The destruction or concealment of public documents is an offense under Article 292 of the Criminal Code[42]. On the other hand, Article 29 of Law 1712 of 2014[43] sets that deliberate concealment, destruction or alteration of all or part of public information, once it has been requested, is a crime under the terms of the above-mentioned article of the Criminal Code.

To comply with the duties hereinabove, Banrep employees must apply the manuals and circulars issued by the General Direction for Information Management and the Document Management Department regarding the management of physical and electronic documents with Banrep information.

Banrep has an Information Management System (SGI)???????[44] for the effective management of its corporate information as well as to ensure its integrity, availability, and confidentiality. Particularly, the SGI Handbook sets that Banrep employees are responsible for taking care of and controlling the information under their responsibility.

Failure to comply with the duties set in the Policies and IT Security Standards entails that the General Direction for Technology Management of Banrep can suspend access to Banrep resources to the employee of Banrep without prejudice of possible disciplinary sanctions resulting from this behavior[45].

4.2 Protection of Personal Data

Information belonging individually and privately to third persons is protected by Article 15 of the Political

Constitution???????[46], which enshrines the right to privacy and *habeas data*.

Law 1266 of 2008 regulates specifically the handling of information stored in databases containing personal data regarding financial, credit, commercial, and service matters.

Law 1581 of 2012???????[47] “which contains general provisions for the protection of personal data” develops the constitutional right of all persons to know, update and rectify information collected on them in databases or archives, as well as their right to privacy. Based on this law and its regulatory norms???????[48], Banrep defined the general policy and guidelines on this matter, according to its functions and services, and as the entity responsible for processing personal data.

According to the Transparency Act described in section 6.1 of this Code, personal data protected by the right to privacy constitutes classified public information. Access to such an information may only be granted in line with the rules set in Laws 1266 of 2008 and 1581 of 2012.

Banrep employees must be aware of and comply with laws 1266 of 2008 and 1581 of 2012, as well as the internal regulations related to the protection of personal data.

4.3 Protection of Information received from other Entities, Corporations, or Persons who are not Banrep employees

As per numeral 5 of Article 38 of Law 1952 of 2019[49], Banrep employees must use classified public information[50] and reserved public information???????[51], exclusively for the purposes to which this information is intended.

For this reason, whenever Banrep employees, in fulfillment of their duties, share information with other entities, corporations, and individuals outside Banrep, must verify **(i)** what information they could share, **(ii)** why they could do so, and **(iii)** what information they could not share.

Banrep employees must properly handle the information they receive from third parties, recognizing whether it is reserved or classified public information and handling it accordingly.

4.4 Misuse of Privileged Official Information

Article 420 of the Criminal Code enshrines the misuse of Privileged Official information as a crime involving any public servant who, as an employee, manager or member of a board or administrative body of a public entity, misuses information known by them due to their functions and that is not the subject of public knowledge, to obtain benefit for themselves or for a third party, which may be a person or a legal entity.

Index

3. Banrep Employees Act with Integrity and Objectivity
4. Banrep Employees Protect Corporate Information and Third-Party Information Held by Banrep
5. Banrep Employees Treat All Persons with whom they relate in their work with Respect, Impartiality, and probity and Create an Inclusive Work Environment
6. Banrep Employees Act Transparently, Denounce, Report Changes in their Judicial Status when Required by Law, and Comply with the Rules on Prevention and Control of the Risk of Money Laundering and Terrorist Financing
7. Other Duties

[38] The Corporate principle for Information Management and its clarifications were approved by the Administrative Council at its meeting of March 22, 2011 and formalized to Banrep employees by the Office of the Governor through Circular Letter GG-435 of July 8, 2011. According to this Circular Letter, corporate information *"(…) corresponds, in general terms, to that which is produced as part of the Bank's processes, activities, services, and operations. Its governance must recognize its value for the institution for being used to support the rights, obligations, responsibilities, decisions, rules, or policies of the Bank as well as the actions taken by its employees or by third parties who provide their services to, and the institutional memory."*

[39] Article 62, numeral 5 of Law 1952 of 2019 states: *"Faults related to public morality: (…) 5. Cause damage to state computer equipment; alter, falsify, introduce, erase, hide or disappear information in any of the official information systems contained therein or in which it is stored, or to allow access to it by unauthorized persons."*

[40] Article 39, numeral 18 of Law 1952 of 2019 provides: *"Prohibitions. All public servers are forbidden to: (…) 18. Give access to or display files, or documents to unauthorized persons."*

[41] Article 38, numeral 6 of Law 1952 of 2019 states: *"Duties. The duties of every public servant are: (…) 6. To maintain and care for the documentation and information under their care or to which they have access because of their employment, position, or function, and to prevent or impede its elimination, destruction, concealment, or improper use."*

[42] Article 292 of the Criminal Code states: "*Destruction, deletion, or concealment of public documents."* *Anyone who destroys, deletes, or hides in whole or in part public documents that may serve as evidence shall incur in imprisonment of thirty-two (32) to one hundred forty-four (144) months.*
If the conduct is carried out by a public servant in the exercise of their functions, they shall be imprisoned for forty-eight (48) to one hundred eighty (180) months and be disqualified for the exercise of rights and public functions for the same term.
If it was a document to be used as evidence in a proceeding, the penalty will be increased from one-third to one-half.

[43] Article 29 of Law 1712 of 2014 states: *"Criminal Responsibility. Any act of total or partial concealment, destruction, or deliberate alteration of public information, once it has been the subject of a request for information, shall be sanctioned under the terms of Article 292 of the Criminal Code."*

[44] The Office of the Deputy Executive Governor formalized and disseminated through Circular Letter GE-1458 of 06 December 2016, the core documents governing the Information Management System (SGI). The basic documents of the SGI are the following: (i) SGI-0001-SGI Manual for the Information

Management System (ii) SGI-002-MSGI-Information Management System Model, and (iii) SGI-003-Glossary of Terms.

[45] Subsection 3.1.5 of the Internal Regulatory Circular DG-T-10 on the duties of persons who provide services to Banrep, provides: *"Failure to comply with the duties set in the Information Security Policies and Standards set out in this circular will result in the suspension of access to computer resources by the Bank's General Direction for Technology Management in coordination with the Director of the Department or Unit, or the General Director, or the Assistant Manager or the Branch Manager, as may be the case, who will further determine whether such conduct (sic) must be reported to the Bank's Internal Control Department, in order to determine the possible occurrence of a disciplinary fault."*

[46] Article 15 of the Constitution provides: *"All people have the right to personal and family privacy and to their good name, and the State must respect them and ensure they are respected. Similarly, they have the right to know, update, and rectify information collected about them in data banks and in archives of public and private entities.*
Collection, processing, and circulation of data shall respect the freedom and all other rights enshrined in the Constitution.
Correspondence and other forms of private communication are inviolable. They can only be intercepted or registered by court order, in cases and with the formalities established by law.
For taxing or judiciary purposes and for cases of inspection, surveillance, and intervention by the State, ledger books and other private documents may be requested, as specified by the law.

[47] Law 1581 of 2012 was partially amended by Decrees 1377 of 2013 and 886 of 2014, which were subsequently incorporated in Decree 1074 of 2015, "*Single Regulatory Decree for the Trade, Industry, and Tourism Sector."*

[48] This law was partially regulated by Decrees 1377 of 2013 and 886 of 2014, incorporated in Decree 1074 of 2015, and by Decrees 1759 of 2016 and 1115 of 2017.

[49] Article 38, numeral 5 of Law 1952 of 2019 provides: "*Duties. The duties of every public server are: (…) 4. To use the assets and resources assigned to them for the performance of their job, position, or function, the powers assigned to them, or the reserved information to which they have access due to their function, exclusively for the purposes for which they are intended."*

[50] According to Article 6, subsection c) of Law 1712 of 2014, classified public information is that which is held or in custody of Banrep, belongs to the private or semi-private sphere of a person or legal entity. For this reason, access to it may be denied or exempted, provided that the circumstances are legitimate and necessary in relation to the individual or private rights enshrined in Article 18 of Law 1712 of 2014.

[51] According to Article 6 subsection d) of Law 1712 of 2014, public reserved information is that which is held or in custody of Banrep, exempted from access by the citizenship due to damages to public interests and under the requirements set in Article 19 of Law 1712 of 2014.