Data Privacy in Bancoob

Karla Castro
Cybersecurity Manager

BANCOOB

Data Privacy in Bancoob

World's Outlook

Brasil
Law 12.965/14 - Civil Framework of the Internet.

Law 13.709/18 - General Data Protection Act Personal.

US Federal Laws

HIPAA, GLBA, COPPA, CAN-SPAM, Do Not Call, Safe Harbor Principle, FCRA

California

California Online Privacy Protection Act 2003, Security Breach Notice (Civil Code 1798 Formerly SB 1386)

Colombia

Personal Data Protection Act 2012

Chile

Private Life Protection Act, Personal Data Protection Act 1998

Argentina

Personal Data Protection Act 2000, Information Confidentiality Law

Canada

PIPEDA, CASL and Provincial Privacy Laws

Switzerland

Federal Data Protection Act 1992

União Europeia (UE)

General Data Protection Regulation (GDPR), Proteção de Privacidade de UE, Diretiva de Retenção de Dados de Comunicação (2006), Diretiva de UE de Privacidade e Comunicações Eletrênicas, implementada por 27 diferentes Leis de Proteção de Dados dos Membros de Estado.

Uruguay

Personal Data Protection Act 2008

Dubai

Personal Data Protection Law 2007

South Africa

Electronic Communications and Transactions Act

India

Legislative proposal under discussion, Information Technology Act 2000

Russia

Federal Law of July 27, 2006, n ° 152-FZ on personal data

South Korea

Law on Promotion of Use of Information and Communication Network, and Data Protection 2000

Taiwan

Protection of Personal Data Processed by Computers

Hong Kong

Personal Data Privacy Decree

Philippines

Data Privacy Act proposed by ITECC, Civil Law of Privacy Law

New Zealand

Privacy Act 1993, Privacy Amendment Act, Privacy Amendment of 1993 and 1994

Australia

Privacy Act 1988, Privacy Amendment Act, Anti-Spam Act - 2004

ONLINE CRIME IN BRAZIL | 2019

1. Branding in digital scams

Everywhere

On the superficial web, branding is the main way to attract victims to fraud and scams. They are everywhere possible.

50,9%
of the cases of piracy and unauthorized sales occurred in the last three months of the year, when happened dates as **Blake Friday** and the **end of year festivities**

only this time, the rate of false profiles grew

31,3%

the rate of branded and similar domains increased

35,1%

These are the two main uses of brands used to publicize and host phising, the most common fraud for ...

2. Capture of sensitive data

Virtual Traps

attracted consumers, the digital frauds steal datas like **passwords, credit and debit cards** simulating sites (cases of phishing) or applications (cases of malware) official.

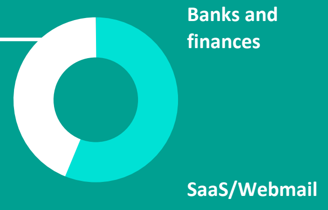
231,5%
was the growth of fake phishing pages between February and December

67%
of phishing attacks are done with brand-name domain names

15 every minutes
A phishing attack were detected in the last trimester

38 Financial Institutions
Diferents (and their customers) were targeted by the same malware, identified in December

E-commerce
Is the sector most affected by phishing, with 44% o
of the total



The same way as system intrusions, these frauds generate...

3. sale and data leak

One key ,many copies

Sensitive data is sold and exposed in lists from the superficial web to the deep web - and generate financial losses for companies

5,7 billions
of exposed credentials* were detected in 2019

23,6 millions
are .br domains

37,6 millions
is the number of times password 123456 was detected in 2019

26,7%
of credit cards leaked online are from Brazil - we are only behind the United States, which has 50.9% of detections

*password or hash email (encrypted password)

Source: AXUR 31/1/2020

Personal Data Privacy Project

Overview

Guardians of privacy and training

71 Privacy guardians (respondents) defined and involved during the project

Privacy Workshops

337 Employees trained on Privacy and LGPD

Risks identified

More than **821** risks in operations identified treatment

Project phases and deadlines

Cybersecurity Diagnosis

- Inventory of personal data (Data Mapping) and Data Discovery
- Identification of risks and threats
- Roadmap and action plan
- Duration: 15 weeks from 1/28/2019 to 5/31/2019

Interviews conducted and scope

95 interviews

(Business, IT and Information Security)

Units evaluated: Torre Z and Aricanduva

Personal Data Privacy Project

Scope

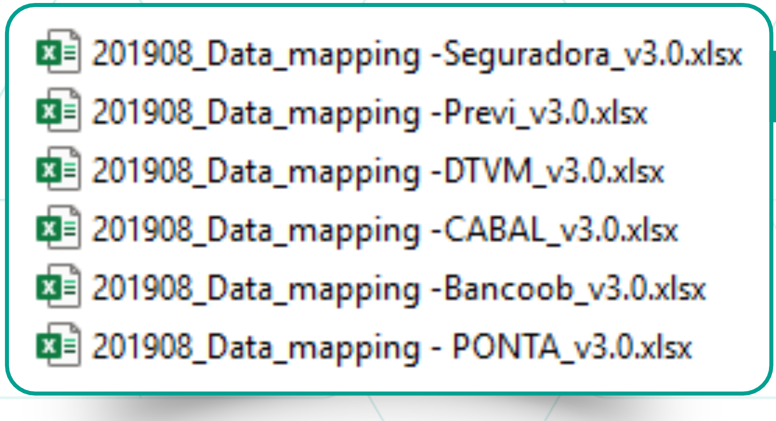
Map the business processes that deal with personal data or sensitive personal data, information security risks / data protection, identification of gaps and recommendations for improvements through an action plan to adapt to LGPD.

1. **Cybersecurity Diagnosis**
2. **Inventory of personal data** (Data Mapping) **and Data Discovery**
3. **Identification of risks and threats**
4. **Action Plan**

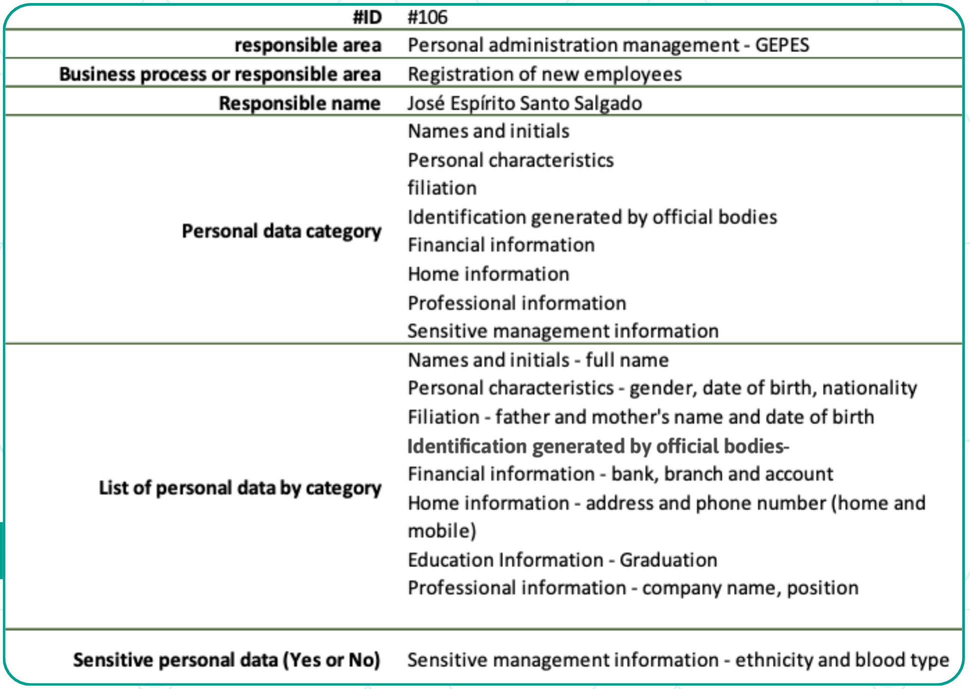
Personal Data Privacy Project

Diagnosis

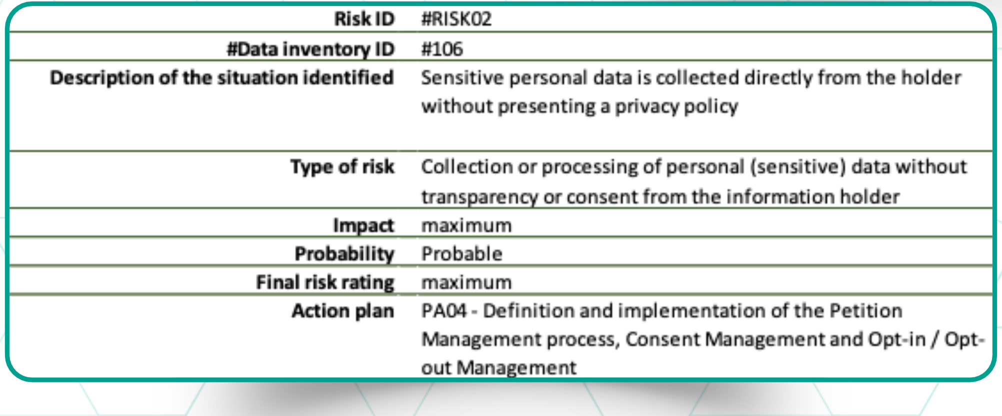
Data Inventory and Identification of Risks and Threats



- 201908_Data_mapping -Seguradora_v3.0.xlsx
- 201908_Data_mapping -Previ_v3.0.xlsx
- 201908_Data_mapping -DTVM_v3.0.xlsx
- 201908_Data_mapping -CABAL_v3.0.xlsx
- 201908_Data_mapping -Bancoob_v3.0.xlsx
- 201908_Data_mapping - PONTA_v3.0.xlsx



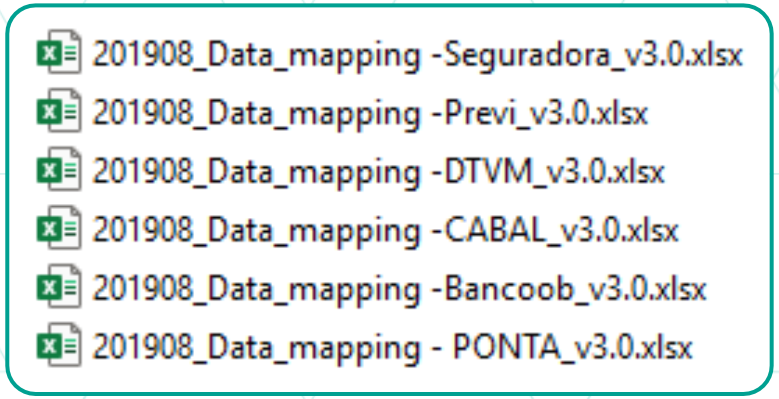
#ID	#106
responsible area	Personal administration management - GEPES
Business process or responsible area	Registration of new employees
Responsible name	José Espírito Santo Salgado
Personal data category	Names and initials Personal characteristics filiation Identification generated by official bodies Financial information Home information Professional information Sensitive management information
List of personal data by category	Names and initials - full name Personal characteristics - gender, date of birth, nationality Filiation - father and mother's name and date of birth Identification generated by official bodies- Financial information - bank, branch and account Home information - address and phone number (home and mobile) Education Information - Graduation Professional information - company name, position
Sensitive personal data (Yes or No)	Sensitive management information - ethnicity and blood type



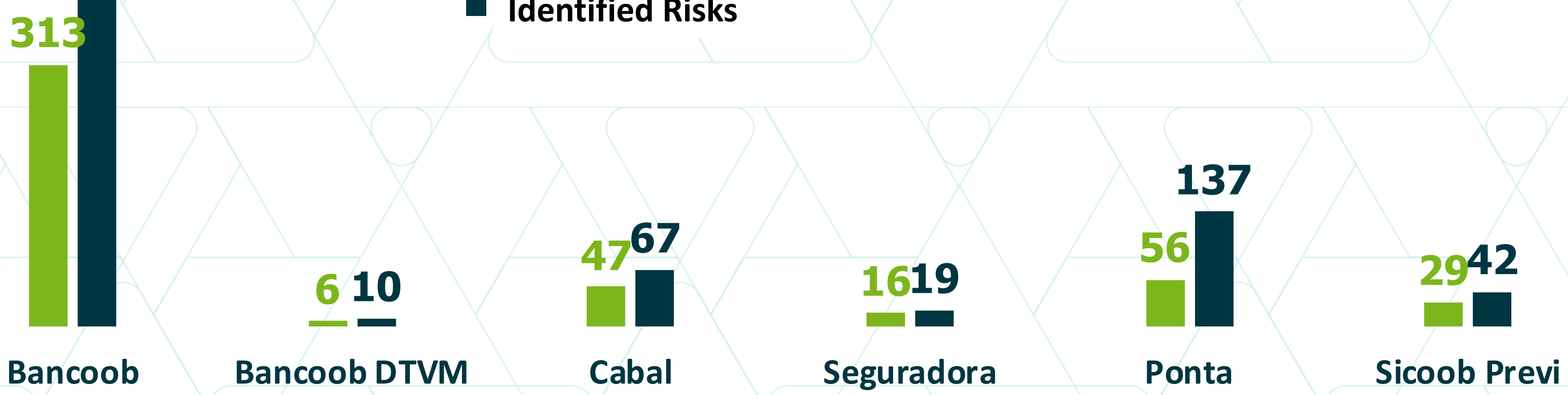
Risk ID	#RISK02
#Data inventory ID	#106
Description of the situation identified	Sensitive personal data is collected directly from the holder without presenting a privacy policy
Type of risk	Collection or processing of personal (sensitive) data without transparency or consent from the information holder
Impact	maximum
Probability	Probable
Final risk rating	maximum
Action plan	PA04 - Definition and implementation of the Petition Management process, Consent Management and Opt-in / Opt-out Management

Personal Data Privacy Project

Diagnosis

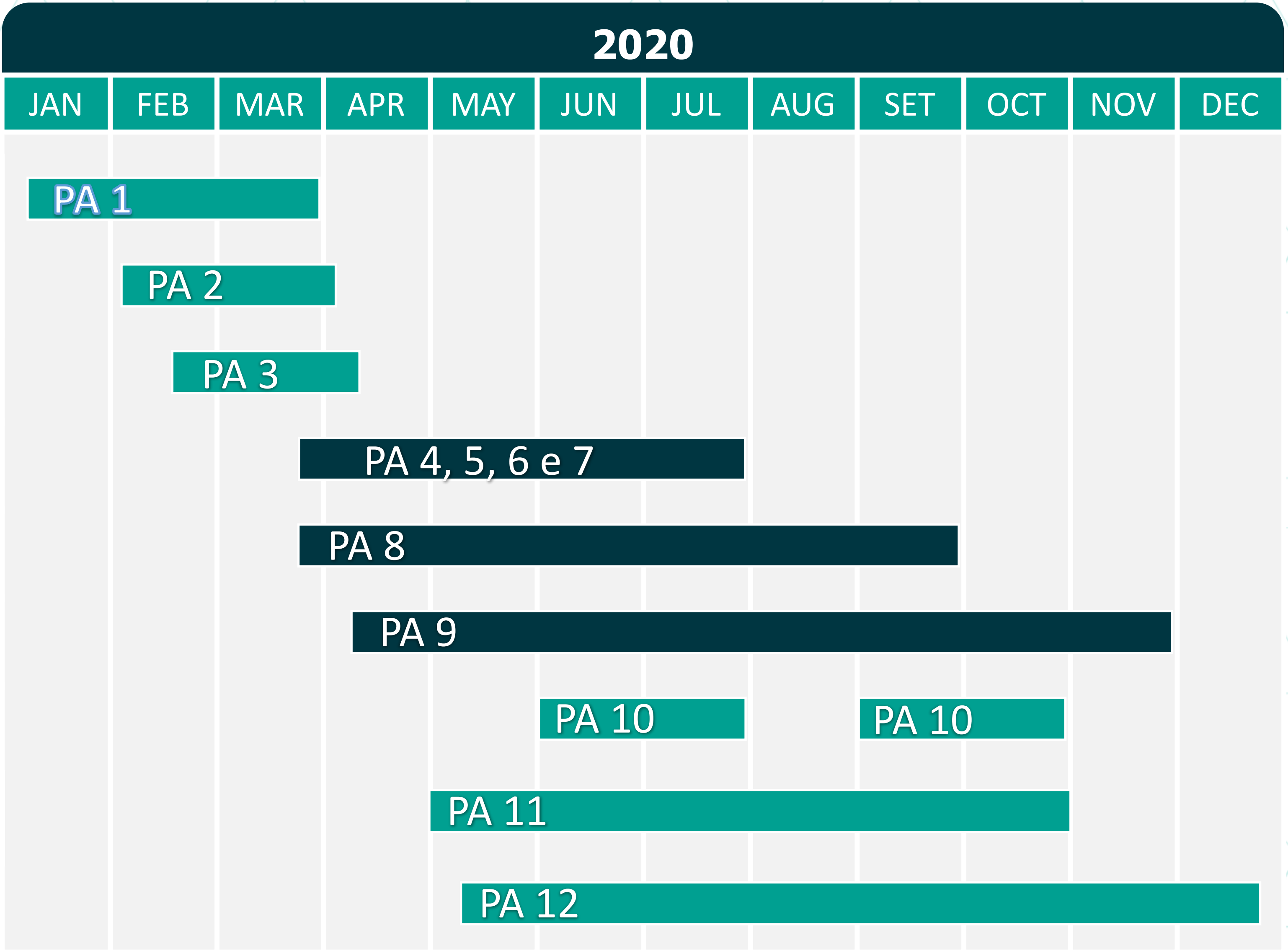


201908_Data_mapping -Seguradora_v3.0.xlsx
201908_Data_mapping -Previ_v3.0.xlsx
201908_Data_mapping -DTVM_v3.0.xlsx
201908_Data_mapping -CABAL_v3.0.xlsx
201908_Data_mapping -Bancoob_v3.0.xlsx
201908_Data_mapping - PONTA_v3.0.xlsx



Personal Data Privacy Project
Action Plan

Governance Structure	Legal Actions
	Organization of privacy and protection of personal data
	Build and approve policies
Structuring Processes	Design of Petitioners, DPIA, PbD and Incidents
	Data Protection in 3rd
	Data Governance
Correction / Adjustments in Existing Processes or Technologies	Training
	Monitoring of personal data via DLP (*Data Loss Prevention*)
	Definition and implementation of access review processes to protect personal data in the systems



Personal Data Privacy Project

Action Plan

PHASE	ACTION PLAN
PA 1 Legal actions for LGPD compliance.	Define legal bases for the treatment of personal data and sensitive personal data.
	Buy personal databases without safeguards for legitimate collection (Serasa and AML).
	Prepare a legal opinion to regularize the collection and treatment of consumers' personal data (Terms of consent).
	Implement Privacy Policy for employees and third parties.
	Review and / or prepare contracts and / or contractual amendments with provision for personal data protection clauses.
	Review contracts for the purpose that are suitable for LGPD.

Personal Data Privacy Project

Action Plan

PHASE	ACTION PLAN
PA 1 Legal actions for LGPD compliance.	Review contract for the purpose of ensuring that personal data is stored in Brazil and otherwise, regularize the situation.
	Review contracts for the purpose that are suitable for LGPD.
PA 2 Definition and implementation of the access review process to protect personal data in the systems.	Appoint a Data Processing Officer.
	Define the role and responsibility of the Data Processing Officer
	Define the competence of the Data Processing Supervisor
	Develop and implement a privacy / data protection governance structure.
	Define an organizational structure with the roles and responsibilities of privacy / data protection at Bancoob.

Personal Data Privacy Project

Action Plan

PHASE	ACTION PLAN
PA 2 Definition and implementation of the access review process to protect personal data in the systems.	Check Bancoob's level of compliance with the General Data Protection Law.
	Creation of a local data privacy portal to disclose the privacy, data retention, storage, sharing and disposal policy
PA 3 Review and implementation of policies and processes to protect personal data.	Add new categorizations, including: personal data and sensitive personal data, collection, handling, storage and disposal of personal data
	Implement policy for secure sharing of personal data
	Implement mobile device usage policy.

Personal Data Privacy Project

Action Plan

PHASE	ACTION PLAN
PA 3 Review and implementation of policies and processes to protect personal data	Develop a policy for sharing with service providers with the best security and privacy practices that must be observed during the contractual relationship with Bancoob.
	Update the cookie policy.
	Update the privacy policy.
	Review the MIG - Cybersecurity.
	Create anonymity procedures.
PA 4 Definition and implementation of the Petition Management process, Consent Management and Opt-in / Opt-out Management	Design a process to meet the requests of the owners (customers, candidates, employees, former employees and service providers).
	Assess consent management tool and Opt-in / Opt-out.

Personal Data Privacy Project

Action Plan

PHASE	ACTION PLAN
PA 4 Definition and implementation of the Petition Management process, Consent Management and Opt-in / Opt-out Management	Define a process for receiving, registering and filing (system), evaluating (confirmation by the holder), escalating and responding to requests.
PA 5 Definition and implementation of DPIA (Risk Assessment)	It is also recommended that a standard response be drawn up for each applicable request type with legal support.
PA 6 Definition and implementation of Privacy by Design	Evaluate tool for managing personal data and DPIA inventory
	Include questions regarding the privacy of personal data
PA 7 Definition of the incident process (inclusion of privacy aspects)	Define a process to communicate the ANPD and the holders in case of privacy incidents that may impact the holders' freedom and privacy.

Personal Data Privacy Project

Action Plan

PHASE	ACTION PLAN
PA 8 Definition and implementation of a personal data protection process in service providers.	Examine the types of risk they pose. Depending on the services provided, the third party may exercise multiple risk factors in the company, which will increase the diligence and guarantee of compliance required from the third party.
	Complete the development of the third-party risk register with a scoring technique to assess and aggregate the risk for each third party individually.
	Monitor, review and report third party risks regularly and be triggered if mergers and acquisitions occur, divestitures, major changes in the organization, entering new markets and geographic expansion.

Personal Data Privacy Project

Action Plan

PHASE	ACTION PLAN
PA 8 Definition and implementation of a personal data protection process in service providers	Develop a risk assessment procedure in the process of contracting third parties with information security questions and a specific chapter to assess privacy in the contracting process, that is, the centralized cybersecurity structure is used.
	To develop the criteria for assessing the security risk of third parties for the company, the inventory must be within the context of the financial sector, the types of services provided and the degree of impact of service dependencies on the organization.

Personal Data Privacy Project

Action Plan

PHASE	ACTION PLAN
PA 9 Definition and implementation of the personal data governance process on the issues demanded by the LGPD.	Implement a process that allows access to a single location of the personal data inventory.
	Build an Information Management model, aiming to structure and mature control over all environments, processes and personal data assets managed by Bancoob, now and in the future.
PA 10 Conducting a corporate data security and protection training program,	Define a personal data protection training plan for Bancoob employees.
PA 11 Monitoring of personal data via DLP (Data Loss Prevention)	Implement rules in the DLP for monitoring personal data.
PA 12 Definition and implementation of the access review process for the protection of personal data in the systems	Review access to systems, network directories that store personal data.

OBRIGADA!

Diretoria de Controle (Dicon)
Superintendência de Gestão de Riscos (Suris)

BANCOOB

OBRIGADA!

Diretoria de Controle (Dicon)

Superintendência de Gestão de Riscos (Suris)