Project name	Solution	Brief description	Year	Main benefit
ISO 27005 Risk Methodology	ISO 27005	Implementation of asset-based risk management methodology, criteria, and treatment aligned with operational risk.	2025	Prioritizing risk treatment based on asset criticality, improving resource efficiency and the effectiveness of security decisions.
Managing Personal Data Risks Online	Risk Controller (Kryptos)	Implementation of a tool that allows for mapping, evaluating, and addressing personal data risks online.	2025	LOPDP/GDPR compliance and privacy risk reduction.
Masking and access control to DB	Guardium Data Protection (IBM)	Implementation of DDM/masking and monitoring of access to sensitive data.	2025	Reducing data exposure and complying with privacy policy.
Definition of Layered Architecture - Defense in Depth	NIST / ISO 27001	Adoption of technical/organizational controls at all layers of defense.	2024	Definition of an architecture that mapped controls and their residual risk by layer. This provided clear visibility into exposure, enabled investment prioritization, and continuously strengthened the bank's security posture.
Secure remote access with SASE/ZTNA	Prisma Access / Palo Alto	Implementing Zero Trust access, inspection, and unified control from the cloud.	2024	Implementation of a SASE model with Prisma Access and MDM, strengthening access control to critical assets and ensuring secure connectivity in the bank's digital transformation.
SOC operational maturity	Cybersoc	Transition of platform and processes to a more refined and complete scheme.	2024	Consolidation of two SOCs into a single CyberSOC with full coverage of critical assets, more than 100 use cases, and a significant reduction in false positives, improving efficiency and comprehensive threat monitoring.
Spine & Leaf architecture for microsegmentation	Aruba	Definition of Spine & Leaf as a basis for microsegmentation.	2024	Strengthening network resilience and containing lateral threats through a secure Spine & Leaf architecture powered by Aruba, improving performance and segmentation in critical environments.
Implementing PAM (Privileged Access Management)	Delinea	Deployment of a PAM tool to strengthen access with critical credentials and privileged sessions with traceability.	2023	Strengthening access control and reducing the risk of privilege misuse, complying with ISO 27001 and NIST CSF frameworks.
NAC Implementation (LAN/Wi-Fi)	ClearPass	Execution of role/device authentication/authorization scheme for LAN and Wi-Fi with granular policies.	2023	Strengthening network security by ensuring that only authorized users and devices access bank resources, eliminating open points and improving traceability and access control under a model of **Zero Trust**.

Project name	Solution	Brief description	Year	Main benefit
Secure SD-WAN Design	Forti	Implementing a secure SDWAN.	2023	Strengthening institutional network resilience, reducing latency, and increasing the availability of critical services by integrating layered security controls and improving traffic visibility under the NIST CSF and ISO 27001 frameworks.
Alternate Site Migration (DRP)	Azure	DR enablement with defined RTO/RPO and periodic switchover testing.	2022	Improving recovery time (RTO/RPO) indicators and ensuring the uninterrupted operation of critical services during crisis events.
Containment of lateral movement in the internal network	FireEye/Trellix	Implementation of controls to prevent the spread of cyberattacks.	2022	Increased capacity for early detection and incident response, reducing the risk of internal spread and containment times.
Patch Deployment Automation with ManageEngine	ManageEngine	Orchestration of the detection→approval→deployment→verification cycle with windows and risk prioritization.	2022	Greater scope and timeliness in patching and timely mitigation of critical vulnerabilities, increasing cyber resilience maturity.
Strengthening account security	Active Directory/Office 365	Redesign of groups/roles/permissions and hardening of authentication and passwords.	2022	Significant improvement in the security of corporate identities and a decrease in incidents due to unauthorized access.
Migrating to EDR/XDR TrendMicro	Trendmicro	EDR/XDR adoption by integrating virtual patching and response playbooks for endpoints/servers.	2021	Greater visibility, early containment and reduced exposure window.