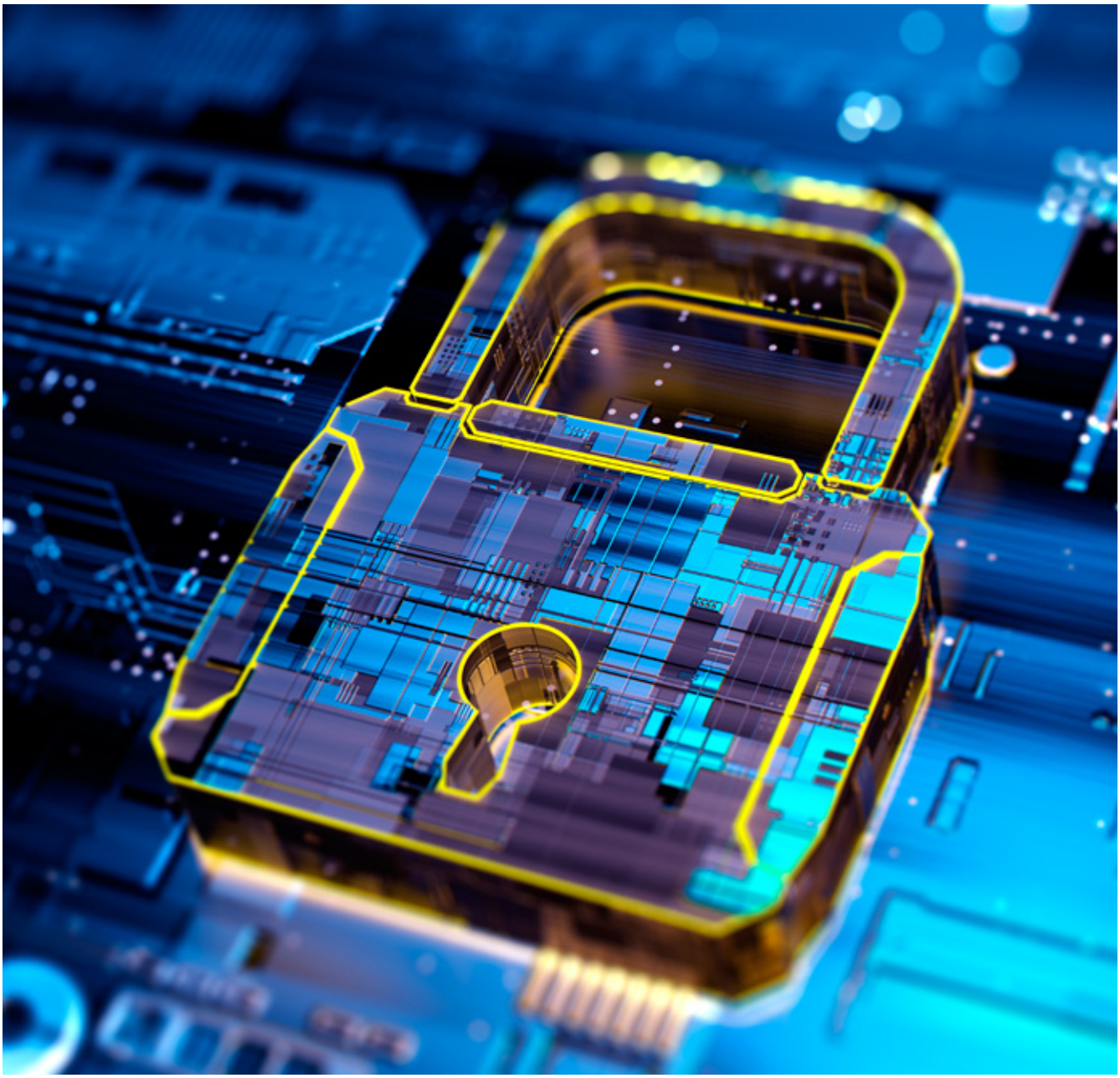
afi

DIGITAL FINANCIAL SERVICES
(DFS) WORKING GROUP

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

CYBERSECURITY FROM THE PERSPECTIVE OF THE FINANCIAL REGULATOR AND SUPERVISORS IN PERU



CASE STUDY

CONTENTS

Acknowledgments

This case study is a product of the Digital Financial Services (DFS) Working Group and its members.

Authors and contributors:
PHB Development expert Simon Priollaud was the lead author of the case study, with support from colleagues David Kleiman and Alexandra Sanchez who contributed to its development. Ghiyazuddin Mohammad (Senior Policy Manager, Digital Financial Services) and Jaheed Parvez (Technical Specialist) from the AFI Management Unit have contributed to the development of the case study.

AFI expresses its warm thanks to Magno Condori from Superintendencia de Banca, Seguros y AFP who truly made the crafting of this case study possible in such challenging times.

AFI is grateful to Superintendencia de Banca, Seguros y AFP for good disposition and collaboration of their team; particularly, to Alejandro Medina, Deputy Superintendent of Risk. AFI also appreciates the support of Luis Daniel Allaín Cañote and Lucero Illary Valderrama from SBS for their valuable insights.
We would like to thank AFI member institutions for generously contributing to development of this publication.

This report is partially funded with UK aid from the UK Government.

Photo by MF3d.

EXECUTIVE SUMMARY

Cybersecurity incidents have increased at a rapid pace in the last decade, affecting all areas of the economy. In the financial sector, the COVID-19 epidemic has been fertile ground for scammers to take advantage of low-income consumers who lack familiarity with tech and the internet marketplace.

The regulatory and supervisory authority of Peru's financial sector, Superintendence of Banks, Insurance Companies, and Private Pension Fund Administrators (SBS), take a very serious view of information security and has been very active in its efforts to improve it over the last decade.

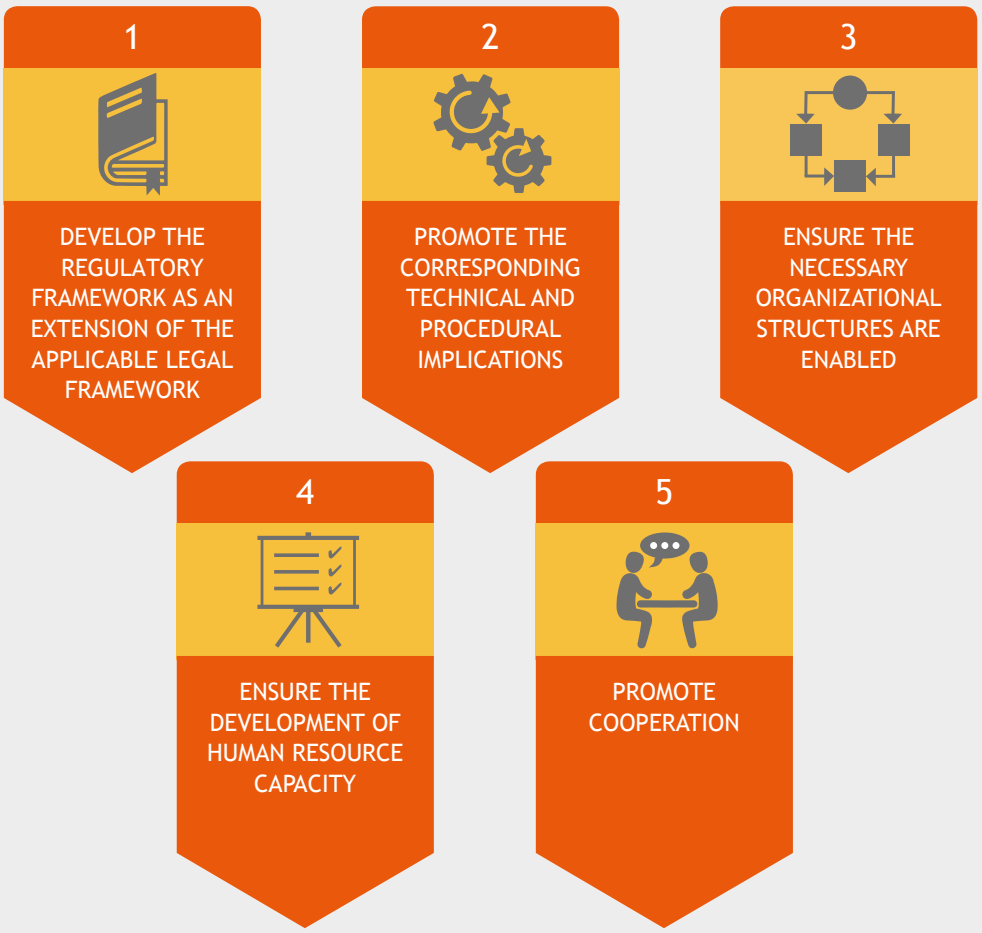
SBS has drawn up its cybersecurity roadmap built on five pillars:

With the implementation of the five pillars below, SBS shows how it is possible to act on cybersecurity and that it is important to consider cybersecurity in the context of its whole ecosystem. As an illustration, universities and other educational bodies have to play a role to prevent the shortage of cybersecurity skills and companies need to retain their talents.

Defining a cybersecurity strategy should not only be about protection against known threats but also the anticipation of future threats and how best to respond to them given the context of the ecosystem.

In most breaches of cybersecurity, the entry point remains the financial institution's employees. Thus, a constant awareness is key for employees from every level, while training is fundamental for those involved in information security management.

FIVE PILLARS IMPROVING THE CYBERSECURITY IN PERU



CHAPTER I - INTRODUCTION

The secure operation of financial services is essential to the stability of the financial system and to promote innovation within it. This is especially true for digital financial services (DFS) because its transactions take place in cyberspace. Cybersecurity is a set of policies, processes, procedures, and resources implemented by an organization to secure its information assets and to rapidly respond to any incidents or breach in order to recover normal operations. As financial institutions in Peru face the challenge of bringing DFS products to market quickly, cybersecurity considerations are commonly a part of their development.

There are several kinds of cybersecurity threats that could harm financial services with serious effects for the financial institution in question and a general loss of confidence in the financial system as a whole. These may include the interruption of critical services and economic and data integrity losses. Consequently, financial institutions must be prepared to deal with cybersecurity incidents that impact them or third parties in the value chain.[1]

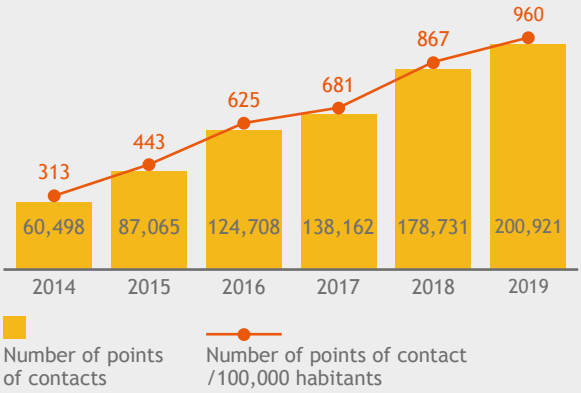
The primary purpose of this document is to show how SBS develops its cybersecurity roadmap and prepares the financial sector, including the insurance and private pension fund industries, to deal with cybersecurity threats or mitigate their effects.

CHAPTER II – CASE STUDY

A. Overview of Peru

Peru has a very active financial system comprising of more than 50 financial services companies. These are mainly comprised of banking and financial institutions and microfinance companies, including municipal and rural savings and loan companies. The Peruvian financial system also includes other types of companies such as issuers of electronic money and investment banks, among others. The number of points of service[2] available in Peru has tripled in the last five years (from 313 to 960 points for every 100,000 adult inhabitants). The measure of financial inclusion, however, was just 34% in June 2019, while the regional average was 51% in 2018.[3] In this context, pre-empting cybersecurity threats will help to maintain public confidence in DFS innovations and to increase financial inclusion by encouraging the widespread adoption of DFS among consumers.

FIGURE 1: NUMBER OF POINTS OF CONTACT AND POINTS OF CONTACT PER 100,000 ADULTS[4]



Peruvians can access financial services over a wide range of channels, including traditional brick and mortar branches, ATMs, correspondent banking outlets and mobile money outlets. This rapid development can be explained by the increasingly important role digital

1 AFI has produced a Cybersecurity for Financial Inclusion: Framework and Risk Guide. AFI, 2019.

2 Including POS, ATM and agents.

3 IFC, Modelo Peru: A Mobile Money Platform Offering Interoperability Towards Financial Inclusion, May 2018. www.ifc.org/wps/wcm/connect/d4960527-29d3-42ae-91e3-488b4011edb2/New+note+54+EMCompass_Note_54-ModeloPeru_FIN+2.pdf?MOD=AJPERES&CVID=mdFTwjZ

4 Reporte de indicadores de inclusión financiera de los sistemas financiero, de seguros y de pensiones, June 2019. www.sbs.gob.pe/inclusion-financiera/cifras/indicadores

channels play in Peru. There has been a proliferation of SIM card usage, from 2,712,000 cards in 2014 to 3,170,000 cards in 2019 and likewise for mobile transactions. Additionally, traditional Peruvian banks and other financial institutions have launched their own mobile banking applications, largely used by their clients.[5] The growing number of digital users (cards and mobile) also means increased cybersecurity risks for the financial sector and consumers.

Peru is one of the first countries to implement a fully interoperable platform that integrates mobile money solutions providers and financial institutions. This initiative was mainly supported by The Peruvian Bank Association (ASBANC), which has been very involved in fostering the growth of DFS. ASBANC's information security committee has actively promoted initiatives to strengthen the cybersecurity[6] of their associated companies.

SBS is in charge of regulating and supervising the financial, insurance and private pension systems (SPP). It is also charged with detecting and preventing money laundering and terrorism financing. Its primary objective is to protect the interests of depositors, policyholders and SPP members that are increasingly exposed to cybersecurity risks.

A1. LEGAL FRAMEWORK

Peru amended its legal framework three years ago by passing the Digital Government Law under which the Digital Government Secretariat of the Presidency of the Council of Ministers (SEGDI) acts as the national authority to promote the digital government framework. Under an emergency decree,[7] Peru also created as part of SEGDI the National Center for Digital Security[8], which is the information exchange and national coordination mechanism that is in charge of the National Registry of Digital Security Incidents. In 2013, Peru added "cybercrime" to its criminal legislative framework and ratified the Budapest convention in 2019 to complement the current regulation.[9]

In addition, Peru has created the National Digital Transformation System[10] to articulate private and public initiatives to achieve the country's objectives of digital transformation and to promote digital innovation.

These legal instruments contribute to reinforcing cybersecurity, and mitigating cybercrime and cyber-attacks, ultimately protecting all Peruvians.

BOX 1: MAIN LAWS ADOPTED AS OF JUNE 2020

- DU No. 007-2020: Digital trust framework and measures to strengthen it, 2020.
- DU No. 006-2020: National digital transformation system, 2020.
- Law No. 30999: Cyber Defense Law, 2019.
- DS No. 10-2019: Ratification of the "Convention on Cybercrime" adopted on November 23rd of 2001 in the city of Budapest Hungary, 2019.
- DL No. 1412: Digital Government Law, 2018.
- DS No. 004-2018-IN: Protection of National Critical Assets – CAN, 2018.

A2. CYBERSECURITY AT THE NATIONAL LEVEL

The National Center for Digital Security, which incorporates the Digital Security Incident Response Team, is the responsible entity in Peru for articulating digital security actions in coordination with other relevant national and international agencies. The National Registry of Security Incidents will receive and maintain data and information on cybersecurity incidents reported by digital services providers in the country. SEGDI, therefore, needs to coordinate cybersecurity efforts with sectoral authorities which in the case of banking, insurance and private pension fund administrators, refers to the Superintendence of Banking, Insurance and AFP.

The main developments in SEGDI up to mid-2020 were focused on digital government regulations for the public sector and several cybersecurity projects. These included the implementation of the National Center for Digital Security and the National Registry of Security Incidents, as well as a platform for cybersecurity information sharing.

5 BCP clients perform more than 40% of their transactions on mobile banking applications while this type of channel is used by 60% of Interbank's clients: iupana.com/2019/08/19/digital-banking-accelerates-in-peru/?lang=en#widget/?lang=en

6 www.asbanc.com.pe/Publicaciones/Memoria-Anual-2019.pdf

7 DU No 007-2020; DU stands for 'Decreto de Urgencia' that could be translated as 'Emergency Decree'.

8 busquedas.elperuano.pe/normaslegales/decreto-de-urgencia-que-aprueba-el-marco-de-confianza-digita-decreto-de-urgencia-n-007-2020-1844001-2/ - article 7

9 www.coe.int/en/web/cybercrime/-/peru-joined-the-budapest-convention-on-cybercrime#:~:text=Peru%20deposited%20the%20instrument%20of,accession%20in%20January%20this%20year.&text=Now%20Peru%20becomes%20the%2064th%20Party%20to%20the%20Budapest%20Convention.

10 DU-006-2020

BOX 2: RESOLUTIONS UP TO JUNE 2020

- Resolution No. 087-2019-PCM: Articles 1 and 2 of Ministerial Resolution No. 119-2018-PCM are amended. Article 1: Creation of the Digital Government Committee. Article 2: Of the functions of the Digital Government Committee, 2019.
- Resolution No. 003-2019-PCM / SEGDI: Creation of the Government Laboratory and Digital Transformation of the State, 2019.
- Resolution No. 005-2018-PCM / SEGDI: Guidelines for the formulation of the Digital Government Plan, 2018.
- Resolution No. 004-2018-PCM / SEGDI: Guidelines of the Leader of Digital Government, 2018.
- Resolution No. 001-2018-PCM / SEGDI: Guidelines for the use of cloud services for entities of the Public Administration of the Peruvian State, 2018.
- DS No. 081-2017-PCM: Formulation of the Transition Plan to the IPV6 Protocol in Public Administration entities, 2017.
- Resolution No. 041-2017-PCM: Mandatory use of the Peruvian Technical Standard NTP-ISO / IEC 12207: 2016, in all the entities that make up the National Computer System, 2016.
- Resolution No. 004-2016-PCM: Mandatory use of the Peruvian Technical Standard ISO NTP / IEC 27001: 2014, in all the entities that make up the National Computer System, 2014.

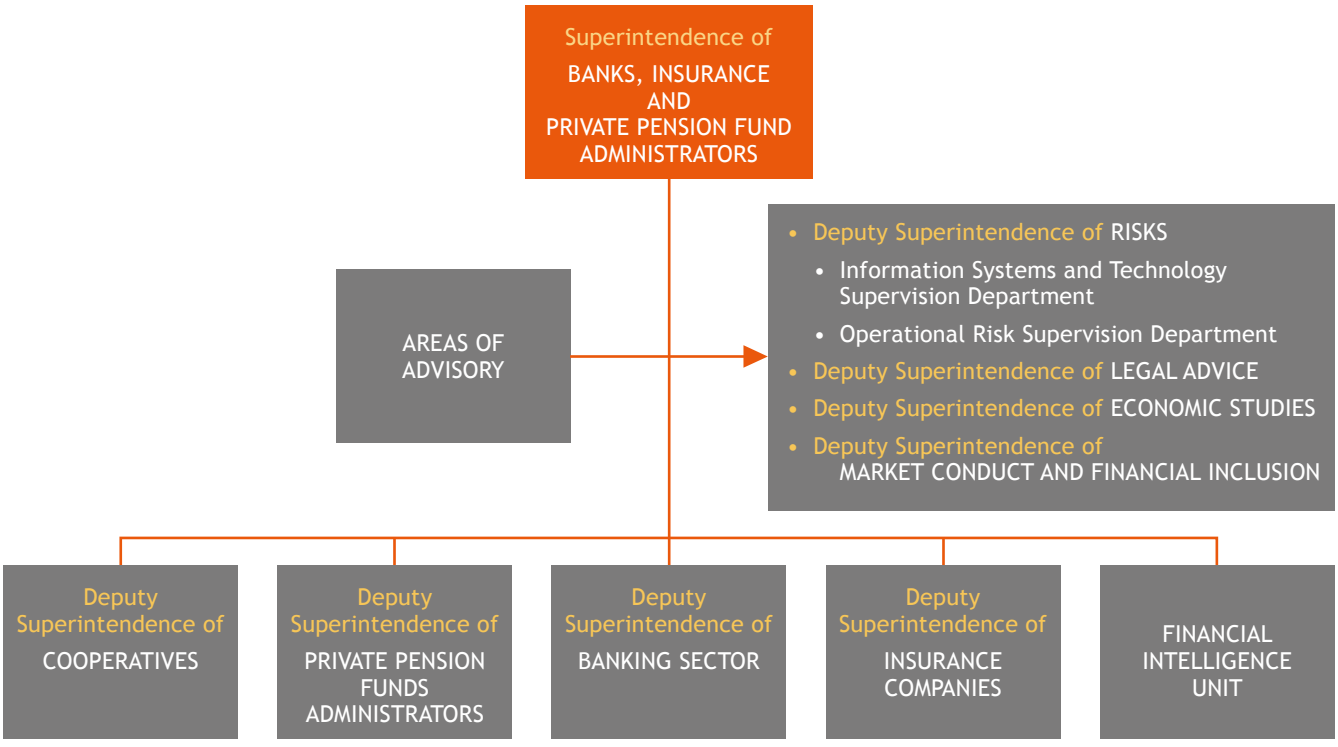
B. THE ROLE OF SBS

The Superintendence of Banking, Insurance and Private Pension Fund Administrators (SBS) is an autonomous institution that is responsible for the regulation and supervision of financial, insurance and private pension systems. SBS's Financial Intelligence Unit is responsible for preventing and detecting money laundering and terrorist financing.

The main objective of SBS is to serve and protect the public interest, i.e. that of depositors, policyholders and private pension fund holders. In order to achieve this goal, SBS carries out four mandates: financial stability, financial integrity, proper market conduct, and security and suitable performance of the private pension system.[11]

B1. ORGANIZATION OF SBS

The senior management of the SBS is strongly engaged internally and externally in the development of cybersecurity capabilities of financial institutions and the digital infrastructure for regulating and overseeing their operational risk management, business continuity management and information security management.



11 More information about the role and mandate of SBS is available at www.sbs.gob.pe/

Regarding the external perspective, which is the focus of this case study, the Deputy Superintendence of Risks (SAR) is responsible for supervising the cybersecurity of financial entities and the supervised systems as a whole.

For this purpose, SAR is composed of:

- Operational Risk Supervision Department, which leads the regulation and supervision of operational risk and business continuity management, and also leads a sectoral Business Continuity Group; and
- Information Systems and Technology Supervision Department, which leads the regulation and supervision of information security and information reliability.

These departments lead cybersecurity development in the course of their supervisory and regulatory activities, working to strengthen the information systems of financial, insurance and private pension fund administrators.

Both departments report to the SAR. At the same time, in the course of their planning, or upon request and before relevant milestones, SBS is also apprised of the status of their current work.

B2. REGULATORY FRAMEWORK

SBS has an existing regulatory framework for risk management by financial institutions to take into consideration any developments in cybersecurity. This regulatory framework comprises of the regulations below, ranging from the general to the specific:

TABLE 1

REGULATORY FRAMEWORK	DESCRIPTION
Corporate Governance and Integral Risk Management	Provides general requirements for the appointments of the board, committees, and different management levels as well as action points to strengthen security (including internal audit and risk management functions). This regulation establishes the need to manage operational risk and pre-requisites for outsourcing services.
Risk report on new products or important changes	Companies must report to SBS the risk evaluation of new products or any important changes to their implementation. This evaluation must include all the kinds of risks that could occur and how to manage them.
Operational risk	Establishes risk management requirements that apply specifically to operational risk. It also establishes that companies must manage information security and business continuity to facilitate operational risk management.
Capital requirement for operational risk	Establishes the methodology to calculate the additional capital requirements for operational risk. Companies must apply one of three prescribed methods.
Criteria to register operational loss events	Sets the criteria to register and maintain an operational loss event database.
Business continuity	Establishes requirements to develop a business continuity plan and implement strategies for any scenario that could affect daily operations.
Significant disruption events report	Establishes reporting requirements for a significant service interruption, including digital financial services. The financial institution must report the interruption, as well as its causes and the measures adopted to restore the service.
Information security management regulation	Requires companies to implement information security measures for access control; personnel security; physical and environmental security; operations and communications administration; acquisition, development and maintenance of information systems; backup procedures; and information security incidents management.

FIGURE 2: INTEGRAL AND OPERATIONAL RISK MANAGEMENT REGULATORY FRAMEWORK

BOX 3: MAIN REGULATION ADOPTED UP TO JUNE 2020

- Res. SBS 877-2020: Business Continuity Management Regulation, 2020.
- Res. SBS 272-2017: Corporate Governance and Comprehensive risk Management, 2017.
- Res. SBS N° 2116-2009: Operational Risk Management Regulation, 2009.
- Res. SBS N° 2115-2009: Capital Requirements for Operational Risk Regulation, 2009.
- Circular SBS G-191-2017 Criteria for recording operational loss events Regulation, 2017.
- Circular SBS G-165-2012: Risk report about New Products / Important Changes Regulation, 2012.
- Circular SBS-G140-2009: Information Security Management Regulation, 2009.

B3. RATIONALE FOR SUPERINTENDENCE OF BANKS, INSURANCE COMPANIES AND PRIVATE PENSION FUND ADMINISTRATORS TO ACT ON CYBERSECURITY

It is worth reiterating that main objective of SBS is to protect the interests of depositors, policyholders, and private pension fund holders. SBS carries out four mandates towards this goal: financial stability; financial integrity; proper market conduct; and security and suitable performance of the private pension system.

Financial services in Peru are subject to a digital transformation process which makes them more reliant on new technologies, third-party providers and connectivity. The financial sector's greater exposure to digital ecosystems means that cybersecurity incidents will have a greater impact on it as DFS becomes more widely adopted. In a critical scenario, a cybersecurity incident can disrupt the operations of a financial institution, reduce public confidence in the financial sector, and damage the availability and integrity of critical services that the financial sector provides.

SBS identifies the objectives of the cybersecurity roadmap as: facilitating the strengthening of cybersecurity capabilities in the supervised system; aiding the development of corresponding efforts from the regulatory and supervisory side; and identifying new developments to pre-empt major cyber incidents, especially those that can escalate and threaten financial stability or harm public confidence with negative effects for financial inclusion.

B4. DEVELOPMENT OF THE CYBERSECURITY ROADMAP

After studying several frameworks on cybersecurity, SBS has adapted the methodology used in the Global Cybersecurity Index (GCI)[12] for its roles as a regulator and supervisor. The GCI was developed by the International Telecom Union (ITU). SBS's cybersecurity roadmap has five pillars which are flexible enough to let the supervision team adjust for new developments.

FIGURE 3: FIVE PILLARS OF THE SBS CYBERSECURITY ROADMAP

FOCUS ON PILLAR 1: Develop specific regulations on cybersecurity as an extension of the integral risk management framework for the financial sector

The objective of this pillar is to establish for supervised entities what is expected of them from a regulatory standpoint, so they can be prepared to deal with a cybersecurity incident.

As explained above, Peru has an existing regulatory framework comprised of regulations for risk management, operational risk management, business continuity, and information security. SBS has issued in February 2021 amendments to these regulations to incorporate cybersecurity requirements, and to strengthen authentication procedures and security requirements for third-party services, including those that use cloud computing.

To encourage financial institutions to develop internal cybersecurity systems, SBS has identified five main areas of focus for the development of regulations:

1 Involvement of senior management to incorporate actions and ensure sufficient resources for cybersecurity development;
2 Integration of cyber risk management as a specialized area of operational risk management;
3 Enhance capabilities of technical and management teams to deal with cyber risk;
4 Ensure the preparedness of a financial institution for a cyber-attack affecting critical services; and
5 Sharing timely information and actions against new threats and vulnerabilities.

Regulation on cybersecurity was issued by SBS in February 2021, which requires a cybersecurity program, authentication processes and security requirements for third party provided services.

Additionally, SBS is working on an additional regulation on cybersecurity incident report.

(Included in the draft regulations are requirements for the authentication for users and third-party services.)

FOCUS ON PILLAR 2: Promote the corresponding technical and procedural implementations

Importantly, technical and procedural implementations let translate the regulatory framework into concrete

12 www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

actions that can be taken by financial institutions to develop their internal cybersecurity capacity so that breaches can be dealt quickly and effectively. Additionally, the authority needs to enable the technical and procedural implementations from its own perspective, as well as financial institutions to deal with those incidents, especially when these could negatively affect users or the financial sector as a whole.

Equally important, these procedural and technical implementations allow SBS to monitor existing and emerging cybersecurity threats and orient its supervision efforts. To this end, SBS is studying the Computer Security Incident Response Team (CSIRT) Services Framework[13] to identify if it is compatible with this role. As part of the study, SBS will also evaluate the use of the Malware Information Sharing Platform (MISP) an open source platform by which organizations can share and store threat intelligence, and collaborate on cybersecurity indicators.[14] Developments as part of this pillar would include coordination with the national incident response team[15] under the National Center for Digital Security.

FOCUS ON PILLAR 3: Ensure the necessary organizational structures are enabled

Financial institutions should integrate their cybersecurity measures into their risk management operations and put in place an adequate organizational structure, otherwise institutions might not enforce the processes for managing cybersecurity threats.

The objective of this pillar is to make sure that a financial institution has the structural capability to anticipate, detect and deal with cybersecurity threats.

The organizational requirements for cybersecurity need to be proportional to the size, nature and complexity of the provider's operations. In general, it includes those needed to develop all functions of the cybersecurity framework described previously.[16]

For instance, the organizational requirement for banks is to have a specialized information security committee. This role could be assumed by the risk committee, whose responsibilities must include: (i) strategic information security planning; (ii) information security management; (iii) evaluating cybersecurity threats; and (iv) reporting any cybersecurity incident. Financial institutions are required to have a multi-disciplinary incident response team.

The organizational structure of SBS is considered adequate for its roles as regulator and supervisor. SBS has a Sectorial Business Continuity Working Group which has so far conducted two sectoral continuity exercises (for a large earthquake scenario) and will conduct one based on a cyber attack that has a major impact on the financial sector.

FOCUS ON PILLAR 4: Ensure the development of human resource capacity

Organizational structures and cybersecurity measures are only as good as the personnel tasked with putting them into effect.

The objective of this pillar is to ensure financial institutions have the human resource capacity to anticipate, understand and rapidly respond to cyberthreats. This objective also applies to the ability of SBS to take appropriate supervisory action in a timely manner.

As with some other jurisdictions, Peru's challenge in developing its cybersecurity capacity is a shortage of technical experts. This stems from a lack of formal programs in educational institutions and shows the need of considering cybersecurity in terms of a holistic ecosystem.

Board of directors are requited to provide resources, establish the organization and define policies on cybersecurity capability developments and to ensure that cybersecurity training requirements are met, and to implement a plan to satisfy them. Additionally, awareness measures and training updates contribute to a better understanding of cybersecurity risks.

Financial institutions are required to provide ongoing training in cybersecurity for all employees. Since 2015, SBS' information systems and technology supervision teams have been given ongoing training in information security and cybersecurity standards, security requirements for credit and debit cards,

13 CSIRT Framework, published by First, Forum of Incident Response and Security Teams, www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

14 MISP describes its functions as, "A threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information … Not only to store, share, collaborate on cybersecurity indicators, malware analysis, but also to use the IoCs and information to detect and prevent attacks, frauds or threats against ICT infrastructures, organizations or people." www.misp-project.org/features.html

15 Equipo de respuesta ante incidentes de seguridad digital del Perú, www.gob.pe/7739

16 Functions taken as a reference from NIST Cybersecurity Framework.

agile methodologies, security controls for ATM, and cybersecurity and digital identity, among other areas.

An understanding of cybersecurity issues allows SBS supervisors to take appropriate action, such as in response to the COVID-19 situation. In this context, SBS's activities included:

> **Assessing the security arrangements for remote work by financial institutions:** Supervisors conducted interviews with financial institutions to assess how they deal with remote work due COVID-19. As a result, a group of institutions was required to evaluate information security risks in their specific remote working environments. A smaller group received an offsite assessment of its security baseline for remote work and provided with cybersecurity monitoring for it.

> **Participating in AFI technical training:** Conducted in February 2020 by AFI for its members, this training session engaged with technical teams across the AFI network on developments in cybersecurity.

> **Issuing supervisory guidance to assess remote work security measures,** which was still unusual until the beginning of the pandemic.

However, despite the achievements, the development of Peru's cybersecurity capacity remains challenging, as it is for almost every other jurisdiction.

FOCUS ON PILLAR 5: Promote cooperation

The objective of this pillar is to promote cooperation among relevant institutions to tackle cybersecurity risks.

SBS recognizes the need for cooperation between all Peruvian financial actors. In that sense, as soon as it is convenient and can be carried out within the current legal framework, the promotion of cooperation agreements with local or international institutions in the field of cybersecurity will be evaluated. In this regard, the studies carried out on the functions of the CSIRT, the notification of cybersecurity incidents and the proof of concept of the information exchange platform will clarify how to develop cooperation in cybersecurity.

Studies show that victims of cyber attacks tend to refrain from reporting them for a number of reasons, the fear of attracting negative attention being the most prominent. In the case of financial institutions, they may be slow to inform customers that their personal data were compromised or are still at risk. Prompt sharing and reporting of cybersecurity incidents by all financial actors would benefit the industry as a whole.

BOX 4: RECOMMENDATIONS BY SBS FOR THE DESIGN AND IMPLEMENTATION OF A CYBERSECURITY STRATEGY FOR THE FINANCIAL INDUSTRY

1 Establish a cybersecurity strategy and adopt a framework for its management, which must be proportional to the size, complexity and risk profile of the organization.

2 Establish a governance structure which includes the establishment of the roles and responsibilities for the implementation and supervision of the effectiveness and efficiency of the strategy and reference framework adopted.

3 Evaluate the risks and controls to allow a prioritized management of said type of risks, starting with the most-exposed services and activities.

4 Monitor the infrastructure and the environment to quickly detect the occurrence of cybersecurity incidents as well as determine the effectiveness of the controls existing in the organization.

5 Respond in a timely manner to cybersecurity incidents, and evaluate their nature, scope and impact. This enables their containment, and facilitates communication and coordination of joint responses with other parties involved.

6 Recover the operations at the same time that the remediation of the incident is carried out, eliminating and correcting the vulnerabilities that caused the incident, as well as communicating it to the relevant parties.

7 Share timely and reliable information among the parties involved, to improve defenses, limit potential harm and increase the level of awareness and learning in organizations.

8 Implement continuous learning and a periodic review of the adopted strategy.

B5. CONSUMER PROTECTION

SBS has observed some modalities where cybersecurity issues could affect consumers in Peru:

- **Phishing** to steal identities and passwords, and cracking of applications, among others. Through different means (e.g. SMS, emails, false links), malicious actors can steal login details to ultimately withdraw funds through cash outs or transfers or use someone's card for online purchases. During the COVID-19 crisis, criminals steal the benefits packages disbursed to the population and enterprises by identifying them from listings and applying for the aid on their behalf.

- **'Log in, apply and withdraw':** With the rising number of transaction types facilitated by online and mobile banking, Peruvians can now easily request for an automated loan disbursement at any time without the need for extensive documentation and KYC requirements. There have been recorded cases of attackers logging into an application or a web page, apply for an automated loan and then transfer the whole amount at once to an out-of-reach account or withdraw the money through an ATM.

In a global context, online scams, phishing and the number of compromised business e-mail accounts are rising due to the economic recession.[17]

To prevent these types of incidents, stronger digital authentication processes are fundamental. Peru's financial sector is working to enhance cybersecurity and enhance the financial and digital literacy of consumers as it understands the reputational risks it faces from cybersecurity threats. New login mechanisms, such as dual authentication with Facebook generator codes, push codes on mobile applications or by SMS and even physical tokens are becoming more common. One barrier to their wider adoption and trust in DFS, however, is the absence of mobile applications in Quechua and Aymara, common local Peruvian languages.

SBS is making efforts to alert customers actively on Facebook through easily understood and visual messages. Proactive measures are key to pre-empt threats to cybersecurity.

Illustrations of some of the messages shared on Facebook to fight against cybersecurity[18]

Photo by 3alexd

17 Global Landscape on COVID-19 Cyberthreats, www.interpol.int/en/content/download/15217/file/Global%20landscape%20on%20COVID-19%20cyberthreat.pdf

18 All the illustrations and messages are available at: www.facebook.com/sbsperu

B6. RESPONSE TO THE COVID-19 PANDEMIC

As of 3 November 2020, Peru was one of the seven countries worldwide most affected by the pandemic with more than 900,000 confirmed cases and more than 34,000 deaths.[19] SBS and financial institutions have implemented remote work regimes and digital channels are used more frequently than before. As part of its communication and awareness campaign, SBS has shared multiple guidance notes over social networks on how to react and stay alert to cybersecurity threats during the pandemic.

Illustration of one of the messages shared on Facebook to fight against COVID-19

B7. RECOMMENDATIONS FOR THE INDUSTRY

From its experience, SBS can share useful insights with regulators from other jurisdictions planning to develop a cybersecurity roadmap.

- Stop-gap and short-term measures are inadequate for cybersecurity. A roadmap is necessary, and global references help in the definition process. These references can include fundamental elements of cybersecurity for financial systems used in G7 jurisdictions, and the methodology found in the Global Cybersecurity Index of the International Telecommunication Union.

- Select a cybersecurity framework such as those by the National Institute of Standards and Technology (NIST) and security standards of the ISO/IEC 27000 series to design the regulatory requirements for financial institutions.

- As part of the regulation drafting process, consider the criterion of proportionality to establish regulatory requirements based on size, complexity or connectivity profile of institutions.

- Integrate the cybersecurity regulatory requirements with the pre-existing risk management regulatory framework. Integration with business continuity or operational risk management requirements are relevant.

- Evaluate what level of visibility, as a financial authority, is necessary and if this visibility influences the supervisory effectiveness of cybersecurity preparedness of financial institutions.

- In the case of a high-impact cybersecurity incident, anticipate how the incident might escalate and what kind of information the authority can and might need to rely on.

- Decide if the information asymmetry that financial institutions and financial authorities suffer relative to cyber criminals needs a coordinated response. Look for an effective information-sharing scheme to make the coordination more effective.

19 Johns Hopkins Center, coronavirus.jhu.edu/map.html

Alliance for Financial Inclusion
AFI, Sasana Kijang, 2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia
t +60 3 2776 9000 **e** info@afi-global.org www.afi-global.org

Alliance for Financial Inclusion AFI.History @NewsAFI @afinetwork