

EXECUTIVE BRANCH MINISTRY OF FINANCE AND PUBLIC CREDIT

Applicable PROVISIONS to the electronic payment funds institutions referred to in Articles 48, second paragraph; 54, first paragraph, and 56, first and second paragraphs of the Law to Regulate Financial Technology Institutions.

EXECUTIVE BRANCH MINISTRY OF FINANCE AND PUBLIC CREDIT

Applicable PROVISIONS to the electronic payment funds institutions referred to in Articles 48, second paragraph; 54, first paragraph, and 56, first and second paragraphs of the Law to Regulate Financial Technology Institutions.

On the margin, a seal with the National Coat of Arms, which reads: United Mexican States.
- FINANCE.- Ministry of Finance and Public Credit.- National Banking Securities Commission.- Banco de México


Banco de Mexico, based on the provisions of the Political Constitution of the United Mexican States, Article 28, sixth and seventh paragraphs; of the Banco de Mexico Law, Articles 24, 26 and 36; of the Internal Regulations of Banco de Mexico, Articles 4, first paragraph; 8 paragraphs 4 and 8; 10, first paragraph, 14 Bis in relation to 17, part I, and 15 in relation to 20 Quater, part IV; of the Agreement of Assignment of the Administrative Units of Banco de Mexico, Article 2, parts VIII and X; of the Law to Regulate Financial Technology Institutions, Articles 48, second paragraph; 54, first paragraph and 56; and the National Banking and Securities Commission, based on the provisions of the Law to Regulate Financial Technology Institutions, Articles 48, second paragraph; 54, first paragraph and 56; of the Law of Credit Institutions, Articles 98 Bis; and of the Law of the National Banking and Securities Commission, Article 4, parts XXXVI and XXXVIII, and 16, parts I and XVII; and

WHEREAS

That in compliance with the General Law of Regulatory Improvement, Article 78, and to reduce the cost of compliance with these provisions, the National Banking and Securities Commission, through a resolution published in the Federal Official Gazette on December 26, 2017, modified the General Provisions applicable to credit institutions to make the term to which multiple banking institutions were subject to constitute their capital requirements for operational risk more flexible;

That on March 9, 2018 was published in the Federal Official Gazette the "Decree issuing the Law to Regulate Financial Technology Institutions and amending and adding various provisions of the Credit Institutions Act, of the Stock Market Law, of the General Law of Credit Organizations and Auxiliary Activities, of the Transparency and Financial Services Arrangement Law, of the Law to Regulate Credit Information Corporations, of the Law for the Protection and Defense of the User of Financial Services, of the Law to Regulate Financial Groups, of the Law of the National Banking and Securities Commission and of the Federal Law on the Prevention and Identification of Transactions with Illegally-Obtained Funds;"

That the Law to Regulate Financial Technology Institutions includes. Within the national financial system framework, to financial technology institutions, while empowering Banco de México and the National Banking and Securities Commission to jointly issue the general provisions to be observed



by electronic payment funds institutions (hereinafter, the Fintech General Provisions.) The principles of financial inclusion and innovation, promotion of competition, consumer protection, preservation of financial stability, and technological neutrality will govern these provisions;


That in order to establish appropriate regulations for electronic payment funds institutions and by the principles outlined in the preceding statement, these general provisions are issued as a unified, systematic, coherent, and transparent regulatory framework that provides legal certainty to participants in the financial technology market. This framework aims to promote the growth of electronic payment funds institutions, protect the interests of their clients, and ensure the overall stability of the financial system.

That in order to guarantee the security of the transactions entered into with clients, the requirements to be met by the authentication of the client and the notification to be made to the client at the time of agreeing or entering into such transactions are established, as well as the terms and conditions of the provision of services through the instruction channels. At the same time, information security requirements are established with respect to such instruction channels to guarantee confidentiality and avoid vulnerabilities in accordance with best practices and international standards.

That to safeguard the sequence of activities and operations carried out by electronic payment funds institutions, it is essential to establish the obligation to have a business continuity plan that must be implemented upon the occurrence of any event that hinders, prevents, or limits the performance of their operations or processes affecting their clients in the event of failures due to unforeseen situations or circumstances. This is reinforced by the obligation to have mechanisms for the management of operational contingencies that reduce the risks to which they are exposed, such as the designation of the person responsible for the administration of contingencies and the necessary certifications on the subject when the referred financial institutions contract the services of third parties to support their operation;

That in the case of those electronic payment funds institutions that have a larger volume of accounts or transactions and carry out their main processes using cloud computing provided by a third party, they must include in their respective continuity plans special measures for prudential reasons to protect the interests of their clients, as well as to maintain the security and operational and financial integrity of such institutions individually, and the security and operational integrity of the payment system as a whole, without prejudice to any other measures imposed by these and other applicable provisions;

That to protect the interests of the clients of electronic payment funds institutions, it is necessary to establish the obligation for these institutions to notify their clients of the existence of information security incidents involving the loss, extraction, elimination, or alteration of their personal or sensitive information, whether in the possession of the electronic payment funds institutions themselves or of third parties that provide them with services, indicating the terms and conditions of such notification, the measures that will be implemented to safeguard the information of the clients and, if applicable, the replacement or substitution of the means of disposition or authentication factors that the electronic payment funds institutions themselves



deem necessary to carry out;

For clients to be aware of the degree of operating efficiency of the electronic payment funds institutions with which they enter into transactions, it is considered relevant to establish that these financial institutions must inform the National Banking and Securities Commission and Banco de México of any operating contingencies lasting at least 30 minutes that occur in any of the client service channels or within the electronic payment funds institution itself, at the same time specifying the elements that must be included in such communication and the term in which it must be made once the operating contingency in question takes place. In addition, and to protect the interests of their clients or users of means of payment, the minimum elements of the notification to be made by these financial institutions when one or more instruction channels are affected as a consequence of these operational contingencies are established.

That in order to provide greater certainty and legal security to the operations of electronic payment funds institutions and thereby protect the interests of their clients, it is considered indispensable to establish the terms and requirements that these financial technology institutions must observe to contract services with third parties and enter into commercial commissions, establishing the cases in which they will require authorization from the National Banking and Securities Commission and Banco de México to enter into such contracts;

That in order to have transparency in the information generated by the relationships that electronic payment funds institutions have with third parties, the characteristics of the list of all their service providers are specified, including the suppliers subcontracted by them, as well as the administrators of commission agents and commission agents, with whom the electronic payment funds institutions have entered into contracts for the provision of services or mercantile commissions, also providing for the dissemination that these financial institutions will give through their web page or mobile application, of the list of the modules or establishments of the commission agents, in which they will indicate the operations and the transaction amounts allowed; and

That in order to ensure transparent, reliable, and comparable financial information for the benefit of electronic payment funds institutions, their clients, and the supervisory functions of Banco de México and the National Banking and Securities Commission, it is necessary to establish a requirement for these financial institutions to contract the services of an independent third party to evaluate their compliance with information security requirements, the use of instruction channels, and operational continuity that they must observe, indicating the characteristics that said independent third party must meet; therefore, they have resolved to issue the following:

Applicable provisions to the electronic payment funds institutions referred to in articles 48, second paragraph; 54, first paragraph, and 56, first and second paragraphs of the financial technology institutions law (hereinafter, the fintech law

CHAPTER I

GENERAL PROVISIONS

CHAPTER II

INFORMATION SECURITY

Section One

Technological Infrastructure vis-à-vis Clients

Section A

Conclusion of contracts through Instruction Channels and Operations through them.

Section B

Authentication in the Instruction Channels

Section C

Information Security Requirements for Instructional Channels

Section Two

Technological Infrastructure in internal processes

Section Three

General Provisions for Technological Infrastructure

CHAPTER III

BUSINESS CONTINUITY

CHAPTER IV

COMMON INFORMATION SECURITY AND BUSINESS CONTINUITY PROVISIONS

CHAPTER V

CONTRACTING OF SERVICES WITH THIRD PARTIES AND COMMISSION AGENTS

CHAPTER VI

INDEPENDENT THIRD-PARTY EVALUATION

CHAPTER VII

SUPPLEMENTARY PROVISIONS

ANNEX 1

Information security indicators.

ANNEX 2

Minimum requirements to develop a Business Continuity Plan.

ANNEX 3

Information Security Incidents.

ANNEX 4

Information Security Incident Report. ANNEX 5 Report on Operational Contingencies.

ANNEX 6

Characteristics of Independent Third Parties.

ANNEX 7

Technical requirements to carry out Operations through Commission agents.

ANNEX 8

Specifications of the information system developed by a third party for the encryption of information shared with the National Banking and Securities Commission and Banco de México.

CHAPTER I GENERAL PROVISIONS

Article 1.- For the purposes of these Provisions, the following terms must be understood, in singular or plural, in addition to the terms used in the Fintech Law:

**Administrator of
Commission Agents:**

Term referring to the person who, as defined in these Provisions, Article 46 organizes a network of commission agents and acts as an intermediary between them and the electronic payment funds institution. Their role is facilitating Operations and services between the commission agents and Clients.

Authentication:

Term referring to the verification of the identity of (i) a Client to allow them to carry out the Operations they require, or (ii) a User of the Technological Infrastructure of the electronic payment funds institution in question to allow them to access, use, or operate any component of such Technological Infrastructure.

Channels of Instruction: Term referring to the equipment, electronic, optical, or any other technological means, automated data processing systems, and telecommunications networks that are part of the Technological Infrastructure of the electronic payment institution in question and allow the Client to conduct Operations through them.

Encryption: Term referring to the mechanism to be used by electronic payment funds institutions to protect the confidentiality of information through cryptographic methods using encryption algorithms and keys.

Cloud Computing: Term referring to the computing services model provided by a third party on-demand and through shared, private, or hybrid infrastructure, regardless of the physical location of the technological infrastructure of the third party. This model may include one or more of the following digital service schemes: infrastructure as a service, platform as a service, or software as a service.

Operational Contingency: Term referring to any event that hinders, limits, or prevents an institution of electronic payment funds from conducting its Operations or those processes that could affect its Clients or the institution of electronic payment funds itself.

Account: Term referring to that accounting record in which the electronic payment funds institution makes, among others, the entries of (a) credits corresponding to (i) the amount of electronic payment funds that it issues in favor of the Client in the name of the person who has opened such record, pursuant to Article 22, part I of the Law, against the receipt of an amount of money, in local currency, or subject to the authorization of Banco de México, in foreign currency, subject to a Fund Transfer, Money Transmission, for receipt of cash or transactions with a Card;(ii) the amount of electronic payment funds subject to the Electronic Payment Funds Transfers received in favor of such Client, as well as (b) charges corresponding to (i) the disposition of electronic payment funds for redemption, subject to a Funds Transfer, payment transactions with any type of means of disposition that the electronic payment funds institution has allowed its Client to make, direct debits, Money Transmittals, or the delivery of cash;

(ii) the amount of electronic payment funds subject to the Electronic Payment Funds Transfers in question.

**Information Security
Event:**

Term referring to any event, internal or external, related, among others, to Clients, third parties contracted by the electronic payment funds institution, persons, or operational processes, as well as to components of the Technological Infrastructure, devices, physical means, or other elements that store information, which constitute any indication of a possible impact on the confidentiality, integrity, or availability of the information that such institution manages or to which it has access in the Technological Infrastructure itself.

Authentication Factor:

Term referring to the Authentication mechanism, based on the physical characteristics of the Client, in devices or information that only the Client possesses or knows, under the terms of these Provisions, Article 5.

Client Identifier:

Term referring to the string of alphanumeric characters, or the information of a device, or any other information known to both the institution of electronic payment funds and the Client holder of the pertinent Account managed by it, which allows to identify it through the Instruction Channel of such institution of electronic payment funds. Among others, the Client Identifier may be the number of the cell phone line that the client uses to access the Instructional Channels, the email address, the number of the client Card, or any other unique identifier associated with the use of the corresponding Instruction Channel.

Information Security Incident:

Term referring to any event, internal or external, related, among others, to Clients, third parties contracted by the electronic payment funds institution, persons, and operational processes, as well as to components of the Technological Infrastructure, devices, physical media, or other elements that store information, which:

- a)** Compromises the confidentiality, integrity, or availability of one or more components of the Technological Infrastructure with an adverse effect on the electronic payment funds institution, its Clients, third parties, suppliers, or counterparties, among others.
- b)** Violate the Technological Infrastructure in such a way as to compromise the information it processes, stores, or transmits.
- c)** Constitutes a violation of information security policies and procedures.
- d)** Constitutes the materialization of an impairment in the institution of electronic payment funds, either by extraction, alteration or loss of the information; by failures derived from the use of the hardware, software, systems, applications, networks and any other channel of transmission of information; by unauthorized access resulting in the improper use of information or systems; by fraud or theft; by an interruption of the activities carried out by the institution itself caused by any action; or by attacks against the interconnected infrastructures known as cyber-attacks.

Personal Information:

Term referring to the combination of the name, surname, and any other element of information that allows the identification of the Client or the recipient of Transfers, such as address, telephone numbers, or e-mail addresses, among others.

Sensitive Information:

Term referring to the combination of the name, surname, or any other piece of information that allows for the identification of the Client or the recipient of Transfers, as well as the information regarding the Identifier of the Client, the Accounts, the respective Card numbers, information relating to previous Operations, and any data that enables Authentication and other relevant details of financial nature.

Management Body:

Term referring to the sole administrator or the board of directors of an electronic payment funds institution, as the case may be.

Business Continuity Plan:

Term referring to the document that integrates the set of strategies, procedures, and actions previously determined by the appropriate institution of electronic payment funds to allow, in the event of Operational Contingencies, the continuity in the Operations, activities, or the performance of the critical processes of such institution of electronic payment funds, or their timely reestablishment, as well as the mitigation of the affectations resulting from such Operational Contingencies.

Security Master Plan:

Term referring to the document that integrates the set of projects determined by the appropriate electronic payment funds institution, to be executed in the short, medium, and long term to establish correct information security management and prevent Information Security Events from materializing into Information Security Incidents.

Strategic Business Continuity and Information Security Policy:

Term referring to the document that includes the strategies of the electronic payment funds institution in terms of business continuity and information security related to its operation following these Provisions, without prejudice to any other element in terms of risk management subject to the general provisions issued by the CNBV under the Fintech Law, Article 48.

Session:

Term referring to the period in which the Client, holder of an Account managed by the electronic payment funds institution, may conduct balance inquiries or consultations of his Operations performed or initiate others once he has entered the Instruction Channel with his Client Identifier.

Card:

Term referring to the means of disposition of the electronic payment funds registered in the Account in question, constituted as the set of data which, when processed by determined systems, allow the initiation of a debit instruction to such Account, different from any other instruction conducted to execute a Transfer.

Third-party Independent:

Term referring to the competent professional to perform evaluation tasks regarding compliance with the requirements that electronic payment funds institutions must comply with under these Provisions, who is external to the electronic payment funds institution, and who complies, as applicable, with the characteristics and requirements set forth in these Provisions, Article 58.

Transfer:

Term referring to the Funds Transfers, Electronic Payment Funds Transfers and Money Transfers, indistinctly or jointly.

Transfer of Funds:

Term referring to the Operation referred to the Fintech Law, Article 22, part III of the between the electronic payment funds institution in question and another electronic payment funds institution, Financial Institution, foreign financial institution, or foreign electronic payment funds institution, according to which the first one makes (i) the credit to an Account for an amount equivalent to the money indicated in the respective order it receives, derived from the charge that such other electronic payment funds institution or entity makes in the corresponding account, or (ii) debiting an Account equivalent to that amount of money that the Client has indicated in the order it issues so that, once the redemption of the referred funds has been made, such amount is credited in favor of the other

institution of electronic payment funds or entity to whom said order is sent for its crediting in the deposit account indicated in the order itself.

For the purposes of this definition, foreign electronic payment funds institutions must be understood as those legal entities located outside the national territory that, in accordance with the applicable legislation in the jurisdiction in question, conduct activities similar to the issuance, administration, redemption and transmission of instruments equivalent to electronic payment funds.

Transfer of Electronic Payment Funds:

Term referring to that Operation referred to in the Fintech Law, Article 22, part II, carried out by the same electronic payment funds institution under the contracts entered into with its Clients for the opening of Accounts, in accordance with which said institution credits a determined amount of electronic payment funds in one of the said Accounts, derived from the charge for such amount in one of the referred Accounts.

Transmission of Money:

Term referring to the Operation referred to the Fintech Law, Article 25, part II, carried out by the electronic payment funds institution authorized to do so.

UDI's:

Term referring to the units of account called "Investment Units" established in the "Decree establishing the obligations that may be denominated in Investment Units and amending and adding various provisions of the Federal Fiscal Code and the Income Tax Law," published in the Federal Official Gazette on April 1, 1995, as amended or added from time to time.

**Technological
Infrastructure User:**

Term referring to the person or component of the Technological Infrastructure of the institution of electronic payment funds, which has the respective authorization to access, use or operate any component thereof. This definition does not include the Clients of the institution of electronic payment funds.

CHAPTER II

INFORMATION SECURITY

Section One

Technological Infrastructure in relation to Clients Section A Conclusion of contracts through Instruction Channels and Operations through them.

Article 2.- Electronic payment funds institutions, when agreeing to enter into Operations and render services through Instruction Channels, must require the express consent of their Clients for such purposes, which may be obtained through the Authentication process referred to in these Provisions, Article 7. In addition, electronic payment funds institutions must:

- I. In the respective contracting, clearly and precisely state the following:
 - a) The Operations and services that may be performed and provided through such Instruction Channels.
 - b) The mechanisms and procedures for Client Authentication, as well as the responsibilities of the Client and the electronic payment funds institution with respect to the execution of Operations and the provision of services through the respective Instruction Channel.
 - c) The mechanisms and procedures for the notification to the Client of the Transactions performed and services rendered by the electronic payment funds institutions through the Instruction Channels.
 - d) The mechanisms and procedures for cancellation of the contracting of services, which must be similar to those of the contracting itself, considering the Client service channels, Client Identification Mechanisms and procedures for Client Authentication.
 - e) The relevant operating restrictions according to the Instruction Channel in question, following the provisions of this Chapter.
- II. To inform its Clients, prior to contracting, the terms and conditions for the use of the Instruction Channels, and to keep such information available for consultation at any time.
- III. To inform its Clients of the risks inherent to the use of the respective Instruction

Channels, as well as to inform them of suggestions to prevent the performance of acts not authorized by them or any other irregular or illegal acts, by which Operations referring to the Accounts of which they are holders may be carried out.

Article 3.- The electronic payment funds institutions, in connection with the Instruction Channels, may:

- I. To allow its Clients to contract additional Operations and services to those originally agreed upon.
- II. Modify the terms and conditions for rendering the previously agreed services that may have a financial impact on their Clients, subject to their express consent, which such institutions may obtain through the Authentication process referred to in these Provisions, Article 7 from the Instruction Channel in question.
- III. Allow its Clients to contract the use of another Instruction Channel, as long as the electronic payment funds institution requires at least one Authentication Factor.

Article 4.- The electronic payment funds institutions must notify their respective Clients, by the means agreed with them and within a period of no more than five seconds, when through Instruction Channels, any of the Operations indicated below are executed or any of the following services are requested to the electronic payment funds institutions:

- I. Transfers and delivery of amounts of money derived from the charge to the Account in question of the Client when the daily accumulated amount of the Operations carried out exceeds the equivalent in local currency of 60 UDI's or when each one individually exceeds the equivalent in local currency of 25 UDI's.
- II. Registration or modification of the means of notification to the Client, in which case the respective electronic payment funds institution must send the notification referred to in this article by the means previously agreed with the Client, as well as by the new means.
- III. Hiring of another service provided through Instruction Channels.
- IV. Deactivation, blocking, reactivation and modification of Authentication Factors.

The electronic payment funds institutions must ensure that the notification sent for this purpose under this article does not contain Personal Information or Sensitive Information of the Client. However, the electronic payment funds institutions must enable mechanisms so that their Clients may, at their choice, receive the Account balance information by virtue of the services provided through the Instruction Channels.

For the purposes of the notification referred to in this article, the electronic payment funds institutions that issue means of disposition must notify both their Clients and the holders of the means of disposition issued.

The electronic payment funds institutions may turn off the notifications when executing any

of the Operations or services provided for in parts I to IV of this Article upon express request of their Clients, which such institutions must obtain through the Authentication process referred to in Article 7 of these Provisions, and having informed their Clients, in advance, of the risks associated with such disabling.

Section B

Authentication in the Instruction Channels

Article 5.- For the purposes of these Provisions, the Authentication Factors to be used by the electronic payment funds institutions may only include information belonging to any of the following categories:

- I. Information that the electronic payment funds institution provides to the Client or allows such Client to generate, under the understanding that only such person knows it, so that it can be entered into the system authorized by the electronic payment funds institution to initiate Session and execute the Operation in question. The Authentication Factors referred to in this part must comply with any of the following schemes:
 - a) Passwords that comply, at a minimum, with the following:
 1. It must consist of at least six consecutive characters and include alphanumeric characters.
 2. In no case, the following information may be used as passwords:
 - i) The Client Identifier.
 - ii). The name or trademark of the electronic payment funds institution.
 - ii). More than three identical characters consecutively.
 - iv) More than three numeric or alphabetic characters in sequential form.
 - b) Questionnaires conducted through electronic messaging channels, call centers or by automated agents, provided they observe the following:
 1. Data that the Client knows and that the electronic payment funds institutions can validate is required, maintaining the due confidentiality of such information.
 2. Defining a set of open questions in questionnaires with at least three questions and an additional question may be posed if one of the answers is incorrect. This set of questions must be unique for each medium through which the questionnaire is submitted, allowing the repetition of only one question among all media. Likewise, randomization mechanisms should be implemented in the presentation of questions to the Client.
In no case may the answers to these questions be data displayed in the

Instruction Channel. Likewise, the information or data of the answer to two or more questions may not be sent by the electronic payment funds institutions to their Clients through the same communication channel, either by printed or electronic means.

3. Validating the answers provided by Clients through computer tools without the operator being able to access the authentication data of the Client. The electronic payment funds institutions must allow their Clients to change the Authentication Factors of this category when the latter so require, under the terms set forth in these Provisions.

Electronic payment funds institutions may use questionnaires to unblock previously blocked Authentication Factors, provided they do so in combination with a second Authentication Factor other than the questionnaire.

- II. Information contained, received, or generated by electronic means or devices that only the Client possesses, including that obtained by devices or applications that create dynamic passwords that the institution provides to the Client, as well as that which allows associating electronic means or devices to a Client through secure mechanisms for the exchange of credentials or cryptographic keys. The foregoing will be subject to the fact that the information is contained, received, or generated in such electronic devices in the sole possession of the Client and complies with the following characteristics:

- a) Have properties that prevent its duplication or alteration.
- b) It is dynamic information that cannot be used on more than one occasion with a validity that may not exceed two minutes, or it is dynamic information generated for the execution of an operation, as well as subsequent operations without any modification, in which case it will be considered, for this subsection, as an independent element to authenticate the operations as authorized by the Client only for the first transaction in which it is used.
- c) It is unknown before its generation and use by officers, employees, representatives of the electronic payment funds institution, or third parties.

The electronic payment funds institutions may provide their Clients with means or devices that generate dynamic one-time passwords that use information from the Operation by means of data capture so that such Passwords may only be used for the requested Operation. In this case, the term provided in paragraph b) of this part will not be applicable.

- III. Information derived from the Client own characteristics, such as those of a biometric nature, fingerprints, hand or face geometry, iris or retina patterns, and voice recognition, among others. For the use of this information, electronic payment funds institutions must have prior authorization from the CNBV and Banco de México.

In any case, two or more Authentication Factors will be considered independent if the

violation of one of the Authentication Factors does not compromise the reliability of the others.

Article 6. -Electronic payment funds institutions may request the CNBV and Banco de México to authorize the use of Authentication Factors referred to in parts I and II of article 5 of these Provisions with characteristics different from those indicated in said article, as well as the use of the information indicated in part III of said article, provided that they certify that the technology used, in the opinion of both Financial Authorities, is reliable to authenticate their Clients.

The application to obtain the authorization indicated in the preceding paragraph must contain the following:

- I. The detailed description of the process, which the Management Body must approve, and the technology used in each part of the process.
- II. The description of the necessary means for transmitting and safeguarding the information to guarantee its integrity, the correct reading of the data, the impossibility of manipulation, and its adequate conservation and availability.

For the case specified in part III of Article 5 of these Provisions, the electronic payment funds institution that applies for authorization referred to in this Article must additionally submit evidence gathered from controlled tests demonstrating that the technological solution and methods used are adequate to authenticate its Clients. Such evidence may be obtained by the same institution of electronic payment funds or by a company specialized in certification of Authentication Factors with the ability to submit reports.

Electronic payment funds institutions must have mechanisms and procedures to ensure that, in the use of the Authentication Factors referred to in part III of article 5 of these Provisions, the information transmitted for the Authentication process is different each time it is generated by incorporating additional information, such as time stamps, random numbers, and counters, among others, in the message encryption process, so that in no case may it be used again or duplicated.

Electronic payment funds institutions must submit the applications for authorization and other information referred to in this Article to Banco de México and the CNBV following these Provisions, Article 59.

Article 7.- The electronic payment funds institutions, in order to allow access to the Instruction Channels, must carry out Client Authentication. In order to perform such Authentication, the electronic payment funds institutions must collect and validate, at least, the following:

- I. The Client Identifier The Client Identifier [sic] and
- II. An Authentication Factor.

The Client Identifier must be unique for each Client and must be associated with all Operations performed by the latter.

Likewise, the electronic payment funds institutions must keep evidence of the Authentication following the provisions of Article 29, part IV of these Provisions.

Article 8.- The electronic payment funds institutions must request, at least, two independent Authentication Factors on each occasion in which the following is intended to be performed:

- I. Registration, cancellation, or any other modification related to the beneficiaries of the Account referred to in the Fintech Law, seventh paragraph of Article 29.
- II. Changes regarding Authentication Factors.
- III. Request for account statements.
- IV. Registration and modification of the means of notification to the Client.

Electronic payment funds institutions will be subject to the provisions of Circular 12/2018 issued by Banco de México in the event they receive claims for unacknowledged charges from their Clients for Operations deriving from any of the transactions described in parts I, II, and IV of this Article.

For the purposes of the provisions of this article, the electronic payment funds institutions may take into account the Authentication Factor used for the initiation of the Session in the Instruction Channels in question.

Article 9.- The electronic payment funds institutions must have policies and procedures to ensure that, in the generation, delivery, storage, unblocking and reestablishment of the Authentication Factors, only the Client will receive, activate, know, unblock, and reestablish them.

In the case of passwords defined or generated by the electronic payment funds institutions during the re-establishment of the Authentication Factors referred to in paragraph a) of part I of Article 5 of these Provisions, the institutions themselves must provide mechanisms and procedures using which the Client must modify them immediately after initiating the corresponding Session when so required according to the type of Instruction Channel and before the execution of any Operation, validating that the Authentication Factors referred to in this paragraph are different from the Authentication Factors referred to in this paragraph must be different from the passwords defined by the electronic payment funds institutions themselves.

Section C

Information Security Requirements for Instructional Channels

Article 10.- The electronic payment funds institutions must establish mechanisms and procedures so that their Clients, when accessing the Instruction Channels, may recognize the institutions themselves. For this purpose, the latter must be subject to the following:

- I. Provide personalized and sufficient information so that Clients can verify, before performing the Authentication procedure, that it is indeed the electronic payment funds institution of which they are a Client. For this purpose, electronic payment funds institutions may use the following information:
 - a) That which the respective Client knows or has provided to the electronic payment funds institution or has agreed with the electronic payment funds institution for

this purpose, such as name, aliases, and images, among others.

- b) That which the respective Client can verify through a means agreed for this purpose with the electronic payment funds institution.
 - II. Once the Client accesses the Instruction Channel in question, the electronic payment funds institution must make available to the Client at least the following information:
 - a) Date and time of the last access to the Instruction Channel in question, and
 - b) First and last name of the Client.

The foregoing will not apply when the Client uses Instruction Channels that do not require prior interaction for the instruction of Operations, such as point-of-sale terminals.

Article 11.- The electronic payment funds institutions must make the necessary provisions so that a third party cannot use the Session once the Client has been authenticated in the Instruction Channel. For purposes of the foregoing, electronic payment funds institutions will establish, at least, the following mechanisms:

- I. Immediately terminate the Session automatically and inform the Client of the reason in any of the following cases:
 - a) When there is inactivity for more than 5 minutes.
 - b) When in the course of a Session, the institution of electronic payment funds identifies relevant changes in the communication parameters of such Session, such as identification of the Instruction Channel, range of addresses of the communication protocols and geographic location, among others, that allow the institution to infer that it could be a theft of a Session.
 - II. Prevent simultaneous access on the same Instruction Channel by using the same Client Identifier and making it known to the Client. Likewise, the electronic payment funds institutions must detect access attempts to the Instruction Channel with incorrect Authentication Factors and, in the event of exceeding three (3) consecutive failed access attempts, they must temporarily restrict access to the Instruction Channel in question, blocking the Authentication Factor of the Client for a period of ten (10) minutes, notifying the Client of such blocking by the means previously agreed with him.

After the ten (10) minutes indicated in the preceding paragraph, the Client may have one (1) more attempt to access the Instruction Channel and, in case an incorrect Authentication Factor is entered, such Authentication Factor will be permanently blocked until the Client performs the unblocking process referred to in Article 9 of these Provisions. The institution of electronic payment funds must notify the Client of this permanent blocking, through the means agreed between the parties.

- III. In the event that electronic payment funds institutions offer third-party services through links, they must inform their Clients that, at the moment of accessing such

services, they will enter another link whose security does not depend on and is not the responsibility of said institution.

In the event that the electronic payment funds institution intends to establish parameters different from those specified in this article, it must obtain prior authorization from Banco de México and the CNBV. Applications for such authorizations must be submitted in accordance with these Provisions, Article 59.

Article 12.- The electronic payment funds institutions, in the use of the Client Identifier and Authentication Factors, must comply with the following requirements:

- I. To have the necessary mechanisms to prevent the reading or presentation in the Instruction Channel of the information provided by the Client and used in the Identification and Authentication Mechanisms.
- II. Ensure that, when at least two Authentication Factors are used, they are independent.
- III. To have procedures to reset the Authentication Factors, in such a way that the Personal Information of the Client or Sensitive Information is not compromised.
- IV. To have procedures to invalidate the Authentication Factors, in order to prevent their use in a service provided by the electronic payment funds institution, when a Client or the electronic payment funds institution itself cancels the use of such service or when the respective Client ceases to be a Client of such institution.

Article 13.- The electronic payment funds institutions may only store information related to the Authentication Factors used by their Clients in the Instruction Channels when such storage is carried out under cryptographically secure protocols, and it is not possible that:

- I. The original Authentication Factors information is obtained from the stored information.
- II. Different data sets generate the same stored information.

Article 14.- Electronic payment funds institutions must establish procedures and mechanisms so that their Clients, who carry out Operations or request the services thereof through Instruction Channels, may at any time temporarily deactivate the performance of such Operations or the rendering of such services, as well as establish procedures to reactivate the use when requested by the Clients.

The electronic payment funds institutions must allow Clients to temporarily deactivate the execution of Operations and the rendering of the services mentioned in the preceding paragraph through the Instruction Channels they have agreed with for such purpose, requesting, at least, an Authentication Factor.

For the reactivation of the execution of Operations and the rendering of services that the electronic payment funds institutions provide through Instruction Channels, such institutions must allow Clients to use the Instruction Channels they agree upon for this purpose, for which they must require at least an Authentication Factor. The electronic payment funds institutions must observe these Provisions, Article 7, to allow access to the Instruction Channel in question once the service has been reactivated.

Section Two

Technological Infrastructure in internal processes

Article 15.- The electronic payment funds institutions, in the case of communications and computing components, must establish the following security aspects:

- I. Logical, or logical and physical, segregation of the different networks into different domains and subnets, depending on the function they perform, or the type of data being transmitted, including segregation of production environments from development and test environments, as well as perimeter and network security components to ensure that only authorized traffic is allowed. In particular, in those segments with links to the outside, such as the Internet, suppliers, authorities, other networks of the electronic payment funds institution or parent company, and other third parties, all referred to those services defined as critical by the institution itself, related, at least with payment systems, Encryption equipment, or Transaction authorizers, among others, must consider secure zones, including the so-called demilitarized zones (referred to as DMZ).
- II. Secure configuration according to the type of component considering, at least, ports and services, inbound and outbound connections to other networks, including the Internet, permissions granted under the principle of least privilege, use of removable storage media, access lists, manufacturer updates and reconfiguration of factory settings. The principle of least privilege must be understood as the enabling of access only to the information and resources necessary for the development of the functions of each User of the Technological Infrastructure.
- III. Security mechanisms in the applications that ensure that, during their execution, they are protected from attacks or intrusions, such as code injection, session manipulation, information leakage and alteration of access privileges, among others. Such mechanisms must be implemented for applications provided by third parties and for applications developed, implemented, and maintained by the electronic payment funds institution.

Article 16. - The electronic payment funds institutions must encrypt the Personal Information and Sensitive Information received, generated, stored, or transmitted in their Technological Infrastructure or that of contracted third parties, as well as the images of identification documents issued by official authorities and biometric information of the Clients, and any other information determined by their policies. In the case of Sensitive Information, the data related to Operations is exempted from Encryption, provided that such data is stored in tables or archives different from those used to keep the rest of the Personal Information and Sensitive Information and that security mechanisms are in place to prevent the integration of such separate archives if not authorized to do so.

The mechanisms and procedures for decrypting the information referred to in this article and the cryptographic keys required for such purpose must be under the exclusive control of the chief information security officer of the electronic payment funds institution in question.

Article 17- The electronic payment funds institutions must have procedures and mechanisms that allow structuring the Personal Information and Sensitive Information stored in the Technological Infrastructure in such a way that the personal data of the Clients cannot be related to the information related to their Operations, including, among others, the amounts, as well as the names or denominations of the recipients or issuers of the payments made by the Clients. This relation can only be generated through computer procedures or applications for consultation, designed by the electronic payment funds institution, which must be executed on demand each time it is necessary to build this relation, either through manual mechanisms or computer systems.

Article 18.- The electronic payment funds institutions, with respect to the information related to the Authentication Factors must comply with the following requirements:

- I. Maintain information security procedures for the custody, distribution, and assignment of the Authentication Factors of its Clients.
- II. Establish procedures and mechanisms so that the information related to the Authentication Factors is not known by any of its officers, employees, or representatives, or by any third party.
- III. Establish procedures and mechanisms that prevent requesting partial or complete information related to the Authentication Factors from its Clients through its officers, employees, representatives, or third parties.

Article 19.- Electronic payment funds institutions must establish procedures and mechanisms to ensure that, when discarding or removing storage components or physical devices, known as hardware, from the Technological Infrastructure, the Client information contained in such components or devices must be irrecoverable.

Article 20.- The electronic payment funds institutions will be obliged to use tools that allow the detection of computer viruses and malicious codes in the Technological Infrastructure, as well as procedures that allow their periodic updating.

Article 21.- The electronic payment funds institutions must perform, before the beginning of their operation and at least every two (2) months, vulnerability scanning tests of all the components of their Technological Infrastructure or that of third parties and contracted commission agents, in which they store, process or transmit information of the electronic payment funds institutions and their Clients. Additionally, in the event of modifications or updates to the Technological Infrastructure, the electronic payment funds institutions must perform vulnerability scanning tests on the updated or modified components before putting the changes mentioned above or updates into production. They must take the necessary actions to remedy, at least, the vulnerabilities classified as critical and high. The CEO or, as the case may be, the sole administrator, will oversee that such tests are carried out through the institution, or a third party contracted for this purpose.

Electronic payment funds institutions must generate a documented remediation plan to address the vulnerabilities detected in the tests mentioned in the previous paragraph, in which their attention must be prioritized according to the criticality of such vulnerabilities, in accordance with the classification made by the institution itself.

Remediation plans referred to in the previous paragraph must be validated by the Chief

Information Security Officer. These plans must, at a minimum, include the designation of the personnel responsible for their implementation and execution, a breakdown of defined activities, start and end dates for these activities, as well as the required technical, material, and human resources. The aforementioned remediation plans must be developed within ten (10) business days following the identification of vulnerabilities and must be made available to National Banking and Securities Commission (CNBV) and Banco de México when these authorities request them.

Article 22.- Electronic Payment funds Institutions must have procedures and mechanisms in place to prevent the installation of any service, application, or software, except for those that:

- I. Are necessary for the operation of the Electronic Payment funds Institution.
- II. Are authorized by the Chief Information Security Officer of the Electronic Payment funds Institution for each element of its Technological Infrastructure.

Article 23.- Electronic Payment funds Institutions with their own infrastructure for operation and information safeguarding must establish procedures and mechanisms to restrict access, both to physical connection ports and peripheral devices, as well as to computer or telecommunications infrastructure.

Likewise, when Electronic Payment Funds Institutions contract with a third party for the necessary infrastructure for their operation and information safeguarding, they must ensure that the third party has the procedures and mechanisms referred to in the previous paragraph.

Article 24.- Electronic Payment Funds Institutions must have robust and secure access control procedures and mechanisms for their Technological Infrastructure, and they must comply with, at a minimum, the following requirements:

- I. Logical access controls for computer and telecommunications infrastructure, as well as their Technological Infrastructure and software infrastructure such as databases, operating systems, and software containers.
- II. Controls for the Management of Technological Infrastructure Users and Passwords.
- III. Controls to ensure the tracking and monitoring of access to systems used for storing Client information, including automatic audits that allow the review of individual access to Client information, actions taken after accessing such information, invalid access attempts, changes to Client Identification and Authentication for data access, and all changes made to the storage system.

If the electronic payment funds institution intends to use practices or standards that do not contain the aforementioned elements, it must obtain prior authorization from the Banco de México and National Banking and Securities Commission (CNBV). To do so, the respective application must be submitted following this Provisions, Article 59. The National Banking and Securities Commission (CNBV) and Banco de México may publish the standards that meet the above requirements on their websites.

Article 25.- Electronic payment funds institutions must establish information security policies that their staff is obliged to observe, including the proper use of resources used for storing Client data, pre-contractual reviews of the profiles of the staff that the electronic payment funds institution intends to hire, as well as risk assessment processes that are carried out at least annually.

Section Three

General Provisions for Technological Infrastructure

Article 26.-Electronic payment funds institutions must establish and document policies and mechanisms to ensure that Instruction Channels only use communication protocols that guarantee the confidentiality of information in point-to-point communication, based on the best international information security practices and standards that, with prior agreement between National Banking and Securities Commission (CNBV) and Banco de México, are published on their respective websites. The encryption mechanisms implemented for these communication protocols must be up to date, free from known vulnerabilities, and ensure strong encryption key lengths.

In the event that an electronic payment funds institution intends to use any practices or standards different from those mentioned above, it must obtain prior authorization from Banco de México and the National Banking and Securities Commission (CNBV). For these purposes, electronic payment funds institutions must submit the applications referred to in this article in accordance with these Provisions, Article 59.

Article 27.-Electronic payment funds institutions must have validation measures to ensure the authenticity of processes executed by different components of the Technological Infrastructure, including operations carried out by Clients, considering at least the following:

- I. Verification of the truthfulness and integrity of information, whether static or in transit.
- II. Authentication between Technological Infrastructure components to ensure that only legitimate service requests are executed from their origin to execution and recording.
- III. Messaging, communication, and encryption protocols, which should ensure information integrity and confidentiality.
- IV. Identification of atypical processes, ensuring that there are monitoring tools or automatic alert measures for their attention by the relevant operational areas.
- V. Updating and maintaining digital certificates and components provided by service providers integrated into the execution processes.

The measures referred to in this article must be established according to the level of risk that electronic payment funds institutions define for each type of process.

Article 28.-Electronic payment funds institutions, for the implementation and development of their computer systems, whether by the institution itself or through a specialized third party contracted for computer program development, must comply with the following:

- I. Document their processes, functionalities, and configurations, including their development or acquisition methodology, as well as the record of changes, updates, and a detailed inventory of each component of the Technological Infrastructure.

The development process must implement information security aspects, at least, in the following stages:

- a) Elaboration of requirements.
 - b) Computer system design.
 - c) Development or acquisition of the computer system in accordance with the design referred to in paragraph b) above.
 - d) Validation of functionalities, purpose, capacity, and quality of the computer system.
 - e) Vulnerability testing and code analysis before its release.
 - f) Release or installation of the computer system.
 - g) Change control in the computer system.
 - h) Secure destruction of information at the end of the life cycle of components or systems.
 - i) In the event that the software is developed by a specialized external company, the electronic payment funds institution must request that the delivered software contains mechanisms to validate its integrity and authenticity at the time of installation in its Technological Infrastructure.
- II. Computer systems must consider the following functionalities throughout their operational process:
- a) Authentication mechanisms between different components used for the operation of the electronic payment funds institution.
 - b) Use of electronic signatures to ensure the integrity and non-repudiation of operational information of the electronic payment funds institution, regardless of whether it is static or in transit.
 - c) Management of Users of the Technological Infrastructure and their privileges.
 - d) Use of encrypted communications for the communication of different computer systems and their components.
- III. Static security review, at least through automated tools, of the security of the computer system every time an update is performed.

Article 29.-Electronic payment funds institutions must maintain the robustness of their Technological Infrastructure, for which they must have:

- I. Controls that allow for an annual review of the components that provide security to their Technological Infrastructure to ensure that they are up to date, and if necessary, update components that are no longer valid.
- II. Procedures and tools for detecting alterations or falsifications of the information

contained in the Technological Infrastructure.

III. Records that allow for monitoring, auditing, and tracking of access and activities carried out by different Users of the Technological Infrastructure of computer systems, regardless of the level of privileges established for their access and the means of communication protocol used. These records must include, at a minimum, the following information:

- a) Date, time, minute, and second of the activities performed by Users of the Technological Infrastructure.
- b) Elements that enable the identification of the User of the Technological Infrastructure performing these activities.
- c) Identification data of the access point used by the User of the Technological Infrastructure to carry out the operation in question.
- d) Internet protocol or similar protocol addresses, depending on the electronic medium used by the User of the Technological Infrastructure.

The generated information must be securely stored for a minimum period of one hundred and eighty (180) natural days and include mechanisms to prevent tampering, as well as maintain internal control procedures for its access and availability.

IV. Records that allow for monitoring, auditing, and tracking of access and activities carried out by different Clients. These records must include, at a minimum, the following information:

- a) Date, hour, minute, and second of the activities performed by the Clients.
- b) Numbers of the Accounts involved in the Transaction, including the Account belonging to the originator of the Transaction, and, if applicable, those of the recipients, and any other information that allows the identification of Transactions carried out by Clients or those who have used the respective disposal means.
- c) Identification data of the Instruction Channel used by the Client or by the user of the respective disposal means to carry out the specific Transaction, as well as the Authentication Factors used for its instruction.
- d) Internet protocol addresses or similar protocol addresses, the phone line number, or other data, in accordance with the Instruction Channel used by the Client or the user of the disposal means.

The generated information must be securely stored for a minimum period of one hundred and eighty (180) natural days from its generation, using previously determined mechanisms to prevent tampering, as well as maintaining internal control procedures for its access and availability.

Such information must be provided to Clients or users of the disposal means who expressly request it from the institution of electronic payment funds through their Client service channels within a period not exceeding ten (10) business days, provided that the Transactions were carried out in the Accounts of Client or user during the one hundred and eighty (180) natural days before

the request for the information in question.

- V. Records that allow for monitoring, auditing, and tracking all operations carried out by computer systems, as well as blocking transmissions that do not meet the established security criteria. These records must include the following:
 - a) Date, hour, minute and second of the activities performed by the computer systems.
 - b) Identification data of the access point used by the computer system to carry out the operation in question.
 - c) Internet protocol or similar protocol addresses, depending on the electronic medium used by the computer system.

The generated information, including that from other sources, must be securely stored for a minimum period of one hundred and eighty (180) natural days, including mechanisms to prevent alteration, and maintain internal control procedures for access and availability.

Article 30.-Electronic payment funds institutions must have a Business Continuity and Information Security Strategic Policy, which their Management Body must approve.

Article 31: Electronic payment funds institutions must have a Security Master Plan, which must be approved by the CEO or, in the absence of one, by the sole administrator. The Security Master Plan must align with the business strategy of the electronic payment funds institution and the Business Continuity and Information Security Strategic Policy and define and prioritize information security projects to reduce exposure to technological risks and the occurrence of Information Security Incidents to acceptable levels as defined by the Management Body based on an analysis of the current situation.

For the approval of the Security Master Plan, the CEO or, if applicable, the sole administrator must ensure that it contains initiatives aimed at improving existing work methods and includes the required controls as per the relevant provisions. Modifications to the Security Master Plan must be approved by the CEO or, if applicable, by the sole administrator.

In the case of electronic payment funds institutions with a CEO and a Board of Directors, the CEO must inform the board of the content of the Security Master Plan and its modifications and must have evidence of approval and implementation.

Article 32.-Electronic payment funds institutions must implement procedures and mechanisms to address Information Security Incidents in their Technological Infrastructure, which include identification, containment, and the proper collection and safeguarding of evidence from such incidents.

Article 33.-Electronic payment funds institutions must evaluate or audit the information security of the Technological Infrastructure at least once a year. Additionally, among the tasks of

this evaluation or audit, electronic payment funds institutions must submit the following documents to the Management Body within the referred period:

- I. A report specifying the level of information security risk to the Technological Infrastructure.
- II. A remediation plan to address observations classified as high and remarkably high criticality found in the aforementioned evaluation or audit.
- III. Evidence of implementing the remediation measures as indicated in the part II of this article.
- IV. Evidence of mitigating the mentioned observations as per the plan mentioned in the part II of this article.

Before commencing operations, electronic payment funds institutions must conduct the evaluation or audit referred to in the previous paragraph on those elements or components of the Technological Infrastructure, whether their own or contracted from third parties, used for the issuance, administration, redemption, or transmission of electronic payment funds, including the services provided to Clients to carry out these activities, as well as the storage of Personal Information and Sensitive Information.

For the purposes of the first and second paragraphs of this article, electronic payment funds institutions using third-party Technological Infrastructure must obtain the following documents from these parties:

- I. Results of the evaluation or audit conducted at least once a year and before commencing operations by these third parties.
- II. A remediation plan to address observations classified as high and remarkably high criticality found in the evaluation or audit mentioned in the previous part I.
- III. Evidence of implementing the remediation plan and mitigating the observations specified in part II of the previous section.

Electronic payment funds institutions must provide the Management Body with the information specified in the previous parts.

The documents referred to in this article must be available for consultation by the Banco de México and National Banking and Securities Commission (CNBV) when requested by the Financial Authorities and, in this case, must be sent as per these Provisions, Article 59.

Article 34.-Electronic payment funds institutions must contract a legal entity with personnel possessing verifiable technical capacity through industry certifications in the field to conduct penetration testing on various systems and applications of the Technological Infrastructure at least every two (2) years. These tests aim to detect errors, vulnerabilities, unauthorized functionality, or any code that poses or may pose a risk to the information and assets of Clients and the electronic payment funds institution itself.

The electronic payment funds institution must send a report with the findings of these tests

to Banco de México and the National Banking and Securities Commission (CNBV) within twenty (20) business days from the date the respective tests have concluded, following these Provisions, Article 59. The CEO must digitally sign the report or, as the case may be, the sole administrator and encrypted following these Provisions, Article 59.

If high or remarkably high criticality observations result from the penetration tests conducted, the respective electronic payment funds institution must submit a documented remediation plan to address these observations to Banco de México and the National Banking and Securities Commission (CNBV) within a period not exceeding twenty (20) business days after the penetration tests have concluded. The CEO must digitally sign the remediation plan or, if applicable, the sole administrator and encrypt it as per these Provisions, Article 59. The National Banking and Securities Commission (CNBV) and Banco de México may comment on the remediation plan anytime.

Upon completing the remediation activities for high or remarkably high criticality observations referred to in the previous paragraph, the electronic payment funds institution must conduct penetration tests again within a period not exceeding two (2) months from the conclusion of these activities to verify the mitigation of the respective vulnerabilities.

Electronic payment funds institutions must document in manuals the methodologies used for classifying the criticality and risk of information security findings, including pen tests and vulnerabilities.

Article 35.-Electronic payment funds institutions must have an individual who, among their responsibilities, serves as the *Chief Information Security Officer (CISO)*. A third party may perform these functions, provided that it complies with the provisions of this article.

The CEO must designate the Chief Information Security Officer or, if applicable, the sole administrator and must not have any conflicts of interest concerning the individual responsible for auditing and information technology functions in the electronic payment funds institution. Moreover, the CISO must not perform functions related to the operation of information security within the electronic payment funds institution.

The Chief Information Security Officer may receive support from representatives of different business units in the exercise of their duties.

Electronic payment funds institutions may designate the CEO or, if applicable, the sole administrator as the Chief Information Security Officer for a maximum period of twelve (12) months from the date they obtain authorization to operate as electronic payment funds institutions.

Article 36.-The Chief Information Security Officer of the electronic payment funds institution must, at a minimum:

- I. Participate in defining and verifying the implementation and ongoing compliance with the information security policies and procedures specified in these Provisions.
- II. Prepare the Security Master Plan, which should, for each defined project, include the project name, objective, scope, start and end dates, areas involved, and the projected investment. The plan referred to in this part must be reviewed and updated at least annually.

- III. Verify, at least annually, the definition of the access profiles to the Electronic Payment Funds Institution Technological Infrastructure, whether it is owned or provided by third parties, following the job profiles, known as functional segregation, including those with high privileges, such as administration of operating systems, databases, and applications.
- IV. Ensure, at least annually or earlier in the event of an Information Security Incident, the correct assignment of access profiles to Users of Technological Infrastructure. The function referred to in this part may be performed by employing representative and random samples.

Likewise, the Chief Information Security Officer will be responsible for the temporary authorization of accesses by exception, such as those of Users of the Technological Infrastructure of development environments with access to production environments, accesses for contingency events, or any other privileged access that does not correspond to the policy determined by the electronic payment funds institution. Likewise, it must be a record containing the name of the Technological Infrastructure User, associated application, environment, the reason for the exception, and the start and end date of the assignment.

- V. Approve and verify compliance with the measures adopted to correct deficiencies detected due to the functions referred to in this Article, parts III and IV, and the findings of internal and external audits related to the Technological Infrastructure and information security.
- VI. Manage information security alerts communicated by the National Banking and Securities Commission (CNBV) or other means, as well as Information Security Incidents, considering the stages of identification, protection, detection, response, and recovery.
- VII. Chair the team formed for detecting and responding to Information Security Incidents in the institution of electronic payment funds.
- VIII. Report to the Management Body, or the audit committee and the risk committee if applicable, in the meeting immediately following, as appropriate, the verification of the Information Security Incident regarding the actions taken and the follow-up of the measures to prevent or avoid the reoccurrence of the aforementioned incidents.
- IX. Verify implementation of annual training programs for all staff, as well as information security awareness programs for Clients, including, if applicable, third parties that provide them with services, which include, among other aspects, activities, and responsibilities of the Technological Infrastructure Users on this matter.
- X. Submit monthly to the CEO or, as the case may be, the management report on information security to the sole administrator. This report must be made to the audit and risk committees or, if absent, to the board of directors of the electronic payment funds institution at the next meeting.

- XI. Consider, at least, the information security risk indicators set forth in these Provisions, Annex 1, and report the result of evaluating such indicators to the Management Body and, if applicable, to the audit committee or risk committee.
- XII. Solve the requirements formulated by Banco de México and the National Banking and Securities Commission (CNBV) and within the institution of electronic payment funds regarding information security.

Electronic payment funds institutions must ensure that the Chief Information Security Officer has the records of the individuals who have access to the information related to the operations in which the electronic payment funds institution is involved, including those located abroad, as well as the Technological Infrastructure Users who have high privileges, such as the administration of operating systems, databases, applications, as well as of their service providers.

Electronic payment funds institutions that belong to a financial group subject to the supervision of the National Banking and Securities Commission (CNBV) or that are part of Consortiums or Business Groups that include a financial entity subject to the supervision of National Banking and Securities Commission (CNBV), may assign the functions of the Chief Information Security Officer to the person who performs such activities in the financial entity supervised by National Banking and Securities Commission (CNBV), provided that such person complies with these Provisions, Article 35.

CHAPTER III BUSINESS CONTINUITY

Article 37.- Electronic payment funds institutions must have a Business Continuity Plan that they must comply with and include the minimum requirements set forth in these Provisions, Annex 2, which must comply with the Strategic Business Continuity and Information Security Policy.

The CEO must approve the Business Continuity Plan or, as the case may be, by the sole administrator, verify that it contains the initiatives to improve the existing working methods following these Provisions. The CEO must approve the modifications to the Business Continuity Plan or, if applicable, by the sole administrator. The CEO must comply with the principles established by the board of directors in the business continuity and information security manual.

In the case of electronic payment funds institutions with a CEO and a board of directors, the former must inform the board of directors of the contents of the Business Continuity Plan or its modifications and have evidence of approval and implementation.

Article 38.- Each institution of electronic payment funds must have the necessary mechanisms for the operational continuity and management of Operational Contingencies of the institution, including their identification, evaluation, monitoring, and mitigation.

Article 39.- The electronic payment funds institutions must have methodologies to estimate the quantitative and qualitative impacts of the possible Operational Contingencies that, in terms of these Provisions, are determined by the person in charge of the administration of Operational

Contingencies for their use in the analysis referred to in these Provisions, Annex 2. The Management Body of each electronic payment funds institution must approve such methodologies with no prejudice to the powers of the CEO to make modifications to the Business Continuity Plan following the principles established by the respective Management Body in the Strategic Business Continuity and Information Security Policy.

Article 40.- The Management Body of the electronic payment funds institution must appoint a person responsible for the administration of Operational Contingencies who

knows the matter and can be appointed as a comprehensive risk manager following the general provisions issued by the National Banking and Securities Commission (CNBV). The person responsible for the administration of Operational Contingencies may be assisted by other areas of the electronic payment funds institution or by third parties contracted for such purpose, specialists in the matter. Such person must have, as a minimum, the following functions:

- I. Prepare, review, and, if necessary, update the Business Continuity Plan.
- II. Evaluate, at least once a year, the scope and effectiveness, as well as compliance with the minimum requirements set forth in Annex 2 of these Provisions, as well as the Business Continuity Plan, established, and report the results of such evaluation to the Management Body and the areas responsible for the critical operating processes, identifying, as the case may be, the necessary adjustments to update, strengthen and comply with them. In the event that the electronic payment funds institution has an audit committee, the functions provided in this part must be performed by such committee.
- III. Coordinate and verify the execution of tests of the functioning and sufficiency of the Business Continuity Plan and report to the Management Body at least once a year on the results of such tests.
- IV. Define and submit to the Management Body the methodology for the administration of Operational Contingencies following the terms established in the provisions corresponding to the administration of operational events. For purposes of the foregoing, the person responsible for the administration of operational events may be assisted by other areas of the electronic payment funds institution itself or by third parties contracted for such purpose, specialists in the matter.
- V. Define and submit the methodologies to estimate the quantitative and qualitative impacts of the Operational Contingencies for approval of the Management Body. For purposes of the preceding, the person responsible for the administration of operational contingencies may be assisted by other areas of the electronic payment funds institution itself or by third parties contracted for such purpose, specialists in the matter.
- VI. Verify the effectiveness of the methodology for estimating the quantitative and qualitative impacts of possible Operational Contingencies at least once a year and, if necessary, correct the methods within the same period. Also, compare its estimates against the Operating Contingencies observed and, if necessary, make corrections.

If the electronic payment funds institutions contract with third parties the services necessary to support their operation, in substitution of the provisions of parts II and III of this article, and only concerning the services rendered by such third parties, the institutions must have documentation evidencing that such third parties have a current certification issued by international standards regarding their capacity to maintain the continuity of their services. The foregoing must be observed with no prejudice to compliance with the provisions of Chapter V of these Provisions.

CHAPTER IV

Common information security and business continuity provisions

Article 41.-Electronic payment funds institutions must maintain a database record of Information Security Events qualified as relevant, Information Security Incidents, Operational Contingencies, as well as failures or vulnerabilities detected in the Technological Infrastructure, including, as appropriate, information related to the detection of failures, operational errors, attempted cyber-attacks, and those effectively carried out, as well as the loss, extraction, alteration, loss or misuse of information of the Users of the Technological Infrastructure or Clients, including the date of the event and a brief description thereof, its duration, service or affected element of the Technological Infrastructure, affected Clients, and amounts, as well as the corrective measures implemented.

The details of the Information Security Events qualified as relevant and Information Security Incidents, as well as Operational Contingencies, must be backed up in the means determined by the electronic payment funds institutions and kept for at least ten (10) years.

Article 42.-In the event of an Information Security Incident, or an Information Security Event in the components of the Technological Infrastructure of the electronic payment funds institution; in the Instruction Channels, or in the technological infrastructure of any third party that affects the operation or the Technological Infrastructure of the electronic payment funds institution, the CEO or, as the case may be, the sole administrator must carry out the following:

Provide the necessary measures to inform Banco de México and the National Banking and Securities Commission (CNBV) immediately of Information Security Incidents using email sent to the email accounts ifpe@banxico.org.mx and Ciberseguridad-CNBV@cnbv.gob.mx, or through other means indicated by Banco de México or National Banking and Securities Commission (CNBV.) Such notification must indicate, at least, the date and time of the beginning of the Information Security Incident in question and, if applicable, the indication of whether it continues or has ended and its duration; a description of such event or incident, as well as an initial assessment of the impact or severity.

In addition, electronic payment funds institutions must send to the email accounts ifpe@banxico.org.mx and Ciberseguridad-CNBV@cnbv.gob.mx or through other means indicated by Banco de México or the National Banking and Securities Commission (CNBV), within five (5) business days following the identification of the Information Security Incident in question, the

information set forth in Annexes 3 and 4 of these Provisions.

In the case of Information Security Events, only those that follow the policies and procedures established by the electronic payment funds institution are considered relevant for having a potential impact on the electronic payment funds institution, its Clients, counterparties, suppliers, or other entities of the financial system, as well as those related to Personal Information or Sensitive Information, images of official identifications and information on Authentication Factors, referred to in part III of article 5 of these Provisions must be reported through the means indicated in the first paragraph of this part. This report must only contain the starting date and time and the description of the event in question.

- I. Conduct an immediate investigation into the causes of the Information Security Incident and establish a work plan describing the actions to be implemented to eliminate or mitigate the vulnerabilities that caused the incident. Such plan must indicate, at least, the personnel responsible for design, implementation, execution, and follow-up; deadlines for its execution, as well as the technical, material, and human resources; and must be sent to Banco de México and the National Banking and Securities Commission (CNBV) no later than fifteen (15) business days after the Information Security Incident was concluded.
- II. When the Information Security Incident consists of Personal Information or Sensitive Information in the custody of the electronic payment funds institution or third parties that provide services to it, was extracted, lost, deleted, altered, or when the electronic payment funds institution suspects that some act was carried out involving unauthorized access to such information, the CEO or, as the case may be, the sole administrator or the person designated by any of them, must notify the Clients of the possible loss, extraction, alteration, loss or unauthorized access to their information, within the following twenty-four (24) hours after the Information Security Incident occurred or became known, through the means of notification that the Client has indicated for such purpose to prevent the risks derived from the misuse of the information that has been extracted, lost, eliminated or altered. Likewise, the Client will be informed of the measures to be taken and, if necessary, the replacement of the corresponding means of disposal or the substitution of the required Authentication Factors.

The notification referred to in this part must include, at least, the nature of the event, its date and time of beginning, duration, and, if any, delimit and indicate the individual effects on each Client. The evidence of this notification must be included in the result of the investigation referred to in this Article, part II.

Article 43.- Electronic payment funds institutions must inform Banco de México and the National Banking and Securities Commission (CNBV) of the Operational Contingencies that occur in any of the client service channels or within the electronic payment funds institution itself by sending an email to the accounts ifpe@banxico.org.mx, contingencias@cnbv.gob.mx, and supervisionfintech@cnbv.gob.mx, or through other means established by Banco de México or the National Banking and Securities

Commission (CNBV), and must generate an electronic receipt. The foregoing provided that such interruptions have a duration of at least thirty minutes.

The notification referred to in the preceding paragraph must be made within sixty minutes after the Operational Contingency in question has taken place and must include the date and time of the beginning of the Operational Contingency, the indication of whether it continues or has ended, and its duration; the processes, systems, and channels affected; a description of the event and an initial assessment of its impact or severity.

Likewise, in the event of an Operational Contingency, the electronic payment funds institution in question must conduct an immediate investigation into the causes that generated the event, and send the results of such investigation to the Mexican Bank and National Banking and Securities Commission (CNBV) within a term not to exceed five (5) business days following the specifications of Annex 5 of these Provisions.

If, as a result of an Operational Contingency, one or more Instruction Channels are affected, the electronic payment funds institution in question must inform its Clients or users regarding the means of withdrawal that is being affected by the Operational Contingency within a period of no more than affected by it, within a term not greater than five (5) seconds counted as of the occurrence of the Operational Contingency and according to the information available at the time of the Operational Contingency, about the intermittence or impossibility of the use of the Instruction Channels, through the means of notification agreed with the Clients or users themselves, and must keep evidence thereof.

In addition to what is provided in the previous paragraph, the electronic payment funds institution must make available to the general public, on the Internet site previously disclosed to its Clients, information regarding the specific Operational Contingency, including, at least, the nature of the event, its date and time of commencement and duration, as well as a general description of the impacts on its Clients, within a maximum period of sixty (60) minutes from the occurrence of the event, and, if applicable, must specify and indicate individual impacts on each Client or user of the channel, which must be communicated to Clients through the means previously agreed for this purpose, within a maximum period of twenty-four (24) hours, starting from the occurrence of the event.

If applicable, the CEO or sole administrator must be responsible for carrying out the provisions of this article.

CHAPTER V

contracting of services with third parties and commission agents

article 44.- Electronic payment funds institutions must require authorization from the Banco de México and the National Banking and Securities Commission (CNBV) to contract the rendering of services with any third party that complies with any of the following characteristics:

- I. Provide services that involve the transmission, storage, processing, safeguarding, or

custody of Personal Information or Sensitive Information, images of official identification documents, or biometric information of Clients, provided that the third party in question has access privileges to access such information or security configuration information, or to access control management.

- II. Carry out processes abroad related to accounting or treasury.
- III. Act as the primary provider of services, the interruption of which, in whole or in part, would prevent the electronic payment funds institution from issuing, managing, redeeming, or transmitting electronic payment funds following the actions referred to in the Fintech Law, Article 22, parts II, III, IV, and V.

Electronic payment funds institutions may only contract the services referred to in the previous parts, as well as any other services when the individuals providing the respective services are obligated to maintain the confidentiality of the information related to the operations conducted with their Clients, as well as the information about these Clients, if they have access to it, at least on the same terms and conditions as electronic payment funds institutions are required to maintain such confidentiality. In any case, the institutions of electronic payment funds will be responsible for violating the confidentiality of the information under their custody or in the control of the referred third parties.

The CEO or, as the case may be, the sole administrator of the electronic payment funds institution must be responsible for approving the contracting of the service providers referred to in this Chapter.

The electronic payment funds institutions must maintain the data of those who provide them with services, in the registry referred to in Article 52 of these Provisions.

The authorization referred to in this article is unnecessary when the electronic payment funds institutions contract with other financial entities subject to the general provisions substantially similar to these Provisions.

Article 45.- Electronic payment funds institutions must submit to the Mexican Bank and the National Banking and Securities Commission (CNBV) a notice twenty (20) business days before the hiring of third parties when such third party:

- I. Function as a secondary or backup provider to complement the operation of a primary provider or guarantee business continuity in case the primary provider is unable to provide the Service, as well as those services whose interruption, partial or permanent, would make it impossible for the institution to issue, manage, redeem or transmit electronic payment funds, according to the acts referred to in Law, Article 22, parts II, III, IV, and V. In such cases, the notice must comply with the requirements in Article 49 of these Provisions.
- II. Corresponds to a financial entity legally empowered and subject to regulation substantially similar to these Provisions at the federal level in financial matters.

Banco de México and National Banking and Securities Commission (CNBV), during the

twenty (20) business days previously referred to, may require the electronic payment funds institution in question that the provision of said service is not carried out through the third party indicated in the notice referred to in this article when either of the two authorities considers that, due to the terms and conditions of the service contract, internal control policies and procedures, or due to the technological or communication infrastructure subject to the service used by said third party, it will not be able to comply with the provisions applicable to the electronic payment funds institution, and, if applicable, the financial stability or operational continuity of the institution itself may be affected, at the discretion of Mexican Bank or the National Banking and Securities Commission (CNBV).

Article 46.- The electronic payment funds institutions may enter into mercantile commission contracts with third parties acting before the general public in the name and on behalf of the respective electronic payment funds institutions only for the performance of the following Transactions:

- I. Cash withdrawals made by the holder Client.
- II. Receipt of cash for credit to own or third-party accounts.
- III. Balance inquiries and account transactions.
- IV. The circulation of instruments for the disposition of electronic payment funds.
- V. Opening of electronic payment funds accounts, observing at all times the Fintech General Provisions referred to in the Fintech Law, Article 58, issued by the Ministry of Finance, or other provisions that may replace it.
- VI. Transfers from electronic payment funds accounts, including payments for services.

For the purposes of this article, electronic payment funds institutions must request authorization from the National Banking and Securities Commission (CNBV) in accordance with the provisions of these Provisions, Article 59.

The transactions provided for in the preceding parts must be carried out in local currency and on behalf of the electronic payment funds institution. If the electronic payment funds institution intends to carry out transactions other than those indicated above through commission agents, it must request authorization from the National Banking and Securities Commission (CNBV) before such transactions, in accordance with the provisions of these Provisions, Article 59.

Those electronic payment funds institutions that carry out the operations indicated in this Article, parts I and II through a credit institution, must be exempted from filing the request for authorization referred to in the preceding paragraph. Additionally, electronic payment funds institutions must at all times comply with the limits established in Fintech General Provisions, Article 9, issued by the National Banking and Securities Commission (CNBV) or any successor regulations and develop monitoring mechanisms in the compliance manual provided for in the Fintech General Provisions, referred to in the Fintech Law, Article 58, issued by the Ministry of Finance, or other provisions that may replace it, to comply with the aforementioned limits.

The electronic payment funds institutions, in the execution of the contracts referred to in this

article, must at all times ensure that the third parties providing them with the services keep the due confidentiality of the information regarding the Transactions entered into with their Clients, as well as the information related to the latter, in case they have access to it.

The CEO or, as the case may be, the sole administrator of the electronic payment funds institution must be responsible for approving the hiring of commission agents.

Article 47.- The electronic payment funds institutions that intend to enter into the merchant commission contracts referred to in the preceding article, must submit the following in the application for authorization:

- I. General operating plan containing the following:
 - a) Detailed description and flow chart of the processes of each of the operations to be contracted considering, if applicable, the reconciliation and settlement process of each of them, the third parties involved and the Technological Infrastructure to be used in the Operation.
 - b) Mechanisms that include the automated controls to be used by the electronic payment funds institution to prevent the commission agents or the Administrator of Commission Agents from exceeding the operation limits set forth in these Provisions, Article 48.
 - c) Mechanisms for monitoring the performance of the commission agent or the Administrator of Commission Agents must consider, at least, the fulfillment of their contractual obligations.

For purposes of the foregoing, the electronic payment funds institution must have plans to evaluate and report to the Management Body or, as the case may be, to the audit committee, the performance of the commission agents or the Administrator of Commission Agents hired and compliance with the applicable regulations related to such hiring.

- d) Technical requirements to carry out operations through commission agents, in accordance with the provisions set forth in Annex 7 of these Provisions.


Electronic payment funds institutions, in order to carry out transactions in addition to those stated in the general operating plan referred to in this part, must request authorization from the National Banking and Securities Commission (CNBV) no later than twenty (20) business days prior to the beginning of the aforementioned transactions. Likewise, when they carry out amendments to such plan that imply substantial changes in the terms under which they would carry out the Transactions with the Clients or users of the means of disposition, they must request authorization from the National Banking and Securities Commission (CNBV) at least twenty (20) business days prior to the date on which they are intended to take effect.

- II. Draft contract, which must indicate the probable date of its execution and the rights and obligations of the electronic payment funds institution and the commission agent or the Administrator of Commission Agents. The contract must also provide for the following:

- a)** Transactions that the commission agent or the Administrator of Commission Agents must carry out on behalf of the electronic payment funds institution.

In the case of Transactions carried out through the Administrator of Commission Agents, the electronic payment funds institutions must provide in the contract the Transactions that the Administrator of Commission Agents will contract on behalf of the electronic payment funds institution with the Commission Agents it will manage, as well as, if applicable, the Transactions and services that the Administrator of Commission Agents will carry out.

- b)** Limits that will apply to each of the Transactions, in accordance with the applicable provisions.
- c)** Rights and obligations that both the electronic payment funds institution and the commission agent or the Administrator of Commission Agents must have, as well as the respective legal consequences and penalties applicable in case of non-compliance with the contract terms.
- d)** Power of the electronic payment funds institution to suspend the execution of operations or terminate the respective contract, both without liability, if the commission agent or the Administrator of Commission Agents fails to comply with the applicable regulations or the contract or presents changes in its operation that affect the conditions of the contracted service.
- e)** Corrective measures that the electronic payment funds institution would implement for non-compliance by the commission agent or the Administrator of Commission Agents with the applicable provisions.
- f)** Prohibition for the commission agent or Administrator of Commission Agents to:
 - 1.** Condition the performance of the transaction on the acquisition of a product or service.
 - 2.** Advertise or promote themselves in any way through stationery or on the front of the receipts provided to Clients on behalf of the electronic payment funds institution.
 - 3.** To carry out the Transactions subject to the commission in terms different from those agreed with the corresponding electronic payment funds institution.
 - 4.** Subcontract the mercantile commission. The provisions of this part must not apply to the Administrator of Commission Agents in the contracting on behalf of and for the account of the institution of electronic payment funds of the commission agents that it will manage, except for those operations and services that the Administrator of Commission Agents itself will perform.
 - 5.** To charge commissions, on its own account, to Clients for the rendering of the services that are the object of the commercial commission, or to receive price or rate differentials with respect to the transactions in which they intervene.

- 
- 6. To carry out transactions with clients on its behalf.
 - 7. To agree exclusively with the institution of electronic payment funds, the performance of the Operations and activities consisting of the receipt of payments for services charged to electronic payment funds accounts.
- g) Proof, within the contract, of the express acceptance by the commission agent or Administrator of Commission Agents of the following obligations:
- 1. Comply with the provisions of the Fintech Law, Article 54.
 - 2. Deliver during the audit and at the request of the electronic payment funds institution, to the independent external auditor of the electronic payment funds institution and to the National Banking and Securities Commission (CNBV) books, systems, records, manuals, and documents, related to the provision of the service in question, as well as to allow the independent external auditor or National Banking and Securities Commission (CNBV) personnel access to its facilities, related to the provision of the service.
 - 3. Inform the electronic payment funds institution of any modification to its corporate purpose or any other change that could affect the operations subject to the contracting at least thirty days before such amendment or change occurs.
 - 4. Keep confidentiality of the information that has been received, transmitted, processed, or stored during the performance of the operations. Likewise, accept that such information may only be used and exploited for the purposes agreed upon in the agreement.
 - 5. Express acceptance of direct responsibility for the improper use of the information of the electronic payment funds institution and, if applicable, to pay indemnities for damages caused by any breach of the provisions of the preceding paragraph.
 - 6. Comply with the terms, conditions, and processes to guarantee to the electronic payment funds institution the transfer, return, and secure disposal of the information subject to the contracted commission when the agreement is terminated.
 - 7. Prevent the improper use of authentication factors by Clients and employees operating the contracted service.
 - 8. Observe the measures to be implemented by the electronic payment funds institution to comply with the Fintech General Provisions, referred to in the Fintech Law, Article 58, issued by the Ministry of Finance, or other provisions that may replace it.

9. Train personnel on conducting Transactions using the commission agent technological infrastructure and information security.

Electronic payment funds institutions must submit to the National Banking and Securities Commission (CNBV) the request for authorization referred to in this article, following these Provisions, Article 59, at least twenty (20) business days before the date on which they intend to carry out the contracting.

The electronic payment funds institutions may empower third parties, through a mandate or commission, to contract in turn with other people in the name and on behalf of the institution itself, the commissions or services referred to in this article, such representatives being designated, for these provisions, as Administrator of Commission Agents.

In this case, the electronic payment funds institutions must establish that it must be the responsibility of the Administrators of Commission Agents to ensure that the commission agents they hire comply with the provisions of this article and Annex 7 of these Provisions.

The provisions of this article must be observed without prejudice to the authorization that may be obtained by the electronic payment funds institution for its Administrator of Commission Agents to be a commission agent.

Article 48.- The electronic payment funds institutions, in carrying out the Transactions through commission agents referred to in these Provisions, Article 46, parts I and II, must be subject to the limits indicated below:

- I. In the case of the Transactions referred to in Article 46, part I, the limit per commission agent may not exceed a daily amount equivalent in local currency to 1,500 UDIs per Client Account.
- II. In the case of the Transactions referred to in Article 46, part II, the limit per commission agent may not exceed a daily amount equivalent in local currency to 4,000 UDIs per Client Account.

Article 49.- The electronic payment funds institutions must attach to the application for authorization referred to in Article 44 or, if applicable, to the notice referred to in Article 45, part I of these Provisions, the following:

- I. Detailed description and flow charts of the processes of the services to be contracted, considering the activities intended to be performed by the electronic payment funds institution, as well as by the service provider; the areas of the electronic payment funds institution itself and the third party involved in the flow of the service; name, description, and functionality of the systems, if any, that will be contracted for the provision of the service, or the systems of the electronic payment funds institution that the respective provider will use.
- II. Draft contract for rendering services, which must indicate the contemplated date of its execution, the rights, and obligations of the electronic payment funds institution and the third party, including the determination of the intellectual property regarding

the designs, developments, or processes used to provide the service. The draft contract must be submitted in Spanish.

Likewise, the express acceptance by the third party of the following obligations must be recorded in the contract:

- a) Comply with the provisions of the Fintech Law, Article 54.
- b) Deliver during the audit and at the request of the electronic payment funds institution, to the Independent Third Party of the electronic payment funds institution itself, as well as to Banco de México and the National Banking and Securities Commission (CNBV), the books, systems, records, manuals, and documents in general, related to the provision of the service in question. Likewise, allow the Independent Third Party or the personnel of Banco de México or the National Banking and Securities Commission (CNBV) access to its offices and facilities, in general, related to the provision of the service in question.
- c) Inform the electronic payment funds institution of any modification to its corporate purpose or any other change that could affect the provision of the service that is the subject of the agreement at least thirty (30) days before such modification or change occurs.
- d) Keep confidentiality of the information that has been received, transmitted, processed, or stored during the provision of the services. Likewise, accept that such information may only be used for the purposes agreed upon in the service provision.
- e) In the event that the third party subcontracts for the partial or total rendering of any of the services rendered to the electronic payment funds institutions, it must notify the institution itself regarding such subcontracting; it must also establish the mechanisms for the subcontracted party to comply with the agreed obligations and provide information for the purposes of these Provisions, Article 52.
- f) Comply with the terms, conditions, and processes for the third party to guarantee to the electronic payment funds institution the secure transfer, return, and disposal of the information subject to the contracted service when it ceases to provide it.
- g) Maintain complete audit logs that include detailed information on accesses or access attempts and the operation or activity performed by Technological Infrastructure . Such records must be available to the authorized personnel of the electronic payment funds institution.
- h) Have access control to the information by the access levels and profiles determined by the electronic payment funds institution.
- i) Allow the electronic payment funds institution to perform the security reviews indicated in these Provisions, Articles 21, 33, and 34, to the contracted services or provide evidence of the performance of these reviews.

III. Documentation with respect to the Technological Infrastructure indicated below:

- a) Description of the communication links the electronic payment funds institution uses to connect with the service provider, including the name of the provider, bandwidth, and type of service provided, among others.
- b) Telecommunications diagram showing the existing connection between each participant in the service provision, such as providers, data centers, and electronic payment funds institution, among others, including redundancy diagrams.
- c) Complete address of where each service will be performed and the primary and secondary data centers where the information will be stored and processed. If the designated place is in national territory, it must include at least the street, exterior and interior number, neighborhood, municipality, zip code, and state. Similar data must be included if the place is located abroad to enable the site to be found with certainty. In the case of Cloud Computing services, only what is indicated in these Provisions, Article 50 must be provided.
- d) If applicable, the scheme of interrelation of applications or systems subject to contracting, including the electronic payment funds institution own systems.
- e) Mechanisms for the continuity of the contracted service.

IV. Mechanisms that will allow the electronic payment funds institution to keep under its safekeeping, either in its own Technological Infrastructure or that of third parties in national territory, the detailed records of all the Transactions carried out, as well as its accounting records, to ensure operational continuity at all times. Such records must be kept in a format that allows consultation, operation, and use, even though the service contracted with the third party is unavailable.

V. Evidence of the controls that the third party will maintain to ensure the confidentiality, integrity, and availability of this information when the third party has access privileges to the images of official identification or biometric information of the Clients.

VI. Description of the mechanisms to monitor the performance of the contracted third party and compliance with its contractual obligations, including, at least, those set forth in these Provisions.

VII. Plans to evaluate and report to the Management Body or, as the case may be, to the audit committee of the electronic payment funds institution, depending on the importance of the service contracted, the performance of the third party, and compliance with applicable regulations related to such service.

VIII. Evidence that allows verifying that third parties have and implement personal data protection and information confidentiality policies that allow the electronic payment funds institution to comply with the legal provisions governing the matter.

In the case of services that are processed, provided, or executed totally or partially outside the

national territory, the electronic payment funds institutions must attach the documentation that proves that third parties reside in countries whose domestic law protects the data of individuals, safeguarding their due confidentiality, or that such countries have signed international agreements with Mexico on such matter or exchange of information between the supervisory bodies, regarding Financial Entities.

In addition, electronic payment funds institutions must:

- a) Have the approval of the Management Body that there will be no impact on the continuity of the operation of the electronic payment funds institution due to the geographic distance and, if applicable, the language to be used in the provision of the service.
- b) Have technical support diagrams that allow solving problems and incidents, regardless of any differences, in time zones and working days.

Likewise, if any authority of the country of origin of the third party referred to in this part requires information related to the services provided to the electronic payment funds institution, the third party must, as soon as legally possible, inform the institution of such request, as well as provide it with a copy of the information delivered to such authority. In this case, the electronic payment funds institution must inform Banco de México and the National Banking and Securities Commission (CNBV) of such a situation in accordance with these Provisions, Article 59, immediately upon becoming aware of it, as well as provide them with a copy of the referred information.

Banco de México and the National Banking and Securities Commission (CNBV) must have a term of twenty-five (24) business days to resolve the request for authorization referred to in this article; once this term has gone by without any pronouncement, the resolution must be deemed to be positive. Any request for additional information from Banco de México or the National Banking and Securities Commission (CNBV) will interrupt the term indicated in this paragraph.

Article 50.- The electronic payment funds institutions, in any case set forth in paragraphs a) and b) of this article, must observe the measures set forth below for reasonable grounds.

The institutions that will be forced to adopt the measures referred to in this article will be those that hire a third party as a primary provider of the services corresponding to Cloud Computing to carry out any of the acts of issuance, administration, redemption, or transmission of electronic payment funds in accordance with the provisions of the Fintech Law, Article 22, parts II, III, IV, and V, when the services provided by such third party, regardless of the nationality of the latter or of the persons exercising Control over it, are susceptible of being interrupted, temporarily or permanently, due to any provision, order, instruction, mandate or equivalent act of a foreign authority directly aimed at preventing, limiting, prohibiting, or blocking the provision of Cloud Computing services by the primary provider, either by the place where the primary provider or the people exercising Control over the primary provider are located or have been incorporated, in which they maintain assets or carry out their operations, as well as by the relationship that such third party has with the respective electronic payment funds institution. This makes it impossible for the institution to carry out the aforementioned acts of issuance, administration, redemption, or transmission of the

aforementioned electronic payment funds.

Electronic payment funds institutions that fall under the situation referred to in the preceding paragraph must include in their respective Business Continuity Plans one of the mechanisms indicated below to guarantee that they will maintain the necessary computing and processing capacity so that, for no more than two hours, the aforementioned mechanisms will be implemented and, at least, the respective processes can be carried out to perform all the issuance, administration, redemption or transmission of electronic payment funds referred to above, during the period of the interruption of the primary Cloud Computing:

A mechanism that, in addition to the primary Cloud Computing referred to in this Article, allows electronic payment funds institutions to count on the availability of Cloud Computing services rendered by a secondary provider, as long as such additional provider is not subject to the same risk to which the primary Cloud Computing is subject, as contemplated in the second paragraph of this Article, by being subject to a jurisdiction other than the jurisdiction in which the risk is giving rise to the interruption of the services provided by the primary provider may occur, as well as by being under the Control of a person other than the primary provider or any other person belonging to the same Business Group of such primary provider or a Group of Persons in which such primary provider or person of the same Business Group participates.

The preceding must not be understood in the sense that the services corresponding to the secondary Cloud Computing must be carried out simultaneously with those of the referred primary Cloud Computing used by the institution in its regular operation, as long as the referred interruption does not occur.

- I. A mechanism that, in addition to the primary Cloud Computing used by the institution in question and place within the case described in the second paragraph of this article, allows the institution in question to have its infrastructure that will enable it to carry out, in a different territory than that of the foreign jurisdiction in which the risk referred to in the second paragraph of this article may occur, the processes referred to in that paragraph, provided that the primary Cloud Computing provider does not carry out such processes or depends on it or the people exercising Control over it, or depends on some other person that both it and those exercising Control over it are subject to the same jurisdiction in which the risk indicated may occur.

The implementation of the mechanism indicated in this part must not imply the simultaneous operation with the Cloud Computing of the primary provider used by the institution in its regular operation as long as the referred interruption does not occur.

- II. Any other mechanism than those contemplated in parts I and II above that, at the request of the electronic payment funds institution, are authorized by Banco de México and the National Banking and Securities Commission (CNBV), regardless of any other authorization that, under these Provisions, Article 44, part III, such authorities grant for the contracting of the primary provider of the Cloud Computing referred to in the

second paragraph of this article, as long as the electronic payment funds institution demonstrates that such mechanism can ensure the continuity in the performance of the acts indicated in the second paragraph of this article, in case the interruption foreseen in such paragraph occurs for the reasons noted therein.

The request for authorization referred to in this part must be submitted following the terms set forth in these Provisions, Article 59.

The electronic payment funds institutions that fall under the provisions of this article must be obliged to comply with the provisions of this article, without prejudice to their power to enter into, under the terms and conditions set forth herein and other applicable provisions, the agreements that allow them to obtain and keep the services related to Cloud Computing provided by third parties in the country or abroad, with computer facilities located within or outside the national territory, in order to carry out the processes corresponding to their Transactions authorized to perform.

The provisions of this article must only be applicable to those electronic payment funds institutions that, as a result of the evaluation made with information at the close of each quarter, are located in any of the following cases:

- a)** During a period of twelve (12) calendar months one of the following activities must be carried out:
 - 1. Make more than three million five hundred thousand Transfer Transactions.
 - 2. Send or receive Transfers for a total amount greater than the equivalent in local currency of six billion UDIs.
- b)** At any time they have had more than one million Accounts which, during a period of twelve (12) consecutive calendar months, have registered, at any time, a positive balance or with respect to which at least one Transfer has been sent during such period, or have had a total balance in the Accounts greater than the equivalent in local currency of four hundred million UDIs.

The electronic payment funds institutions to which this article is applicable must have a term of one hundred and eighty (180) calendar days from the first day of the calendar month immediately following the month in which the event referred to in paragraphs a) or b) above occurs, as the case may be, to comply with the provisions of this article.

Article 51.- Electronic payment funds institutions, for the contracting of services with third parties that are subject to authorization in terms of these Provisions, Article 44, as well as those related to operating processes and administration of databases and computer systems, must comply with the following:

- I.** In the case of third parties that provide services related to operational processes and administration of databases and computer systems, consider these Provisions, Article 47, part II, subpart g), paragraphs 1 to 6, and keep the respective agreement.
- II.** At least annually, perform internal or external audits on the contracted service or have

evidence that the contracted third party carries them out.

- III. Maintain in its offices where the administration functions of the electronic payment funds institution are performed at least the documentation and information related to the evaluations, audit results, and, if applicable, the corresponding work plans, as well as the performance reports of the third parties hired, including documentation regarding compliance with the Provisions, part I of this article.
- IV. Update the respective description or documentation when there are amendments considered to have a relevant impact on the service provided or related to the systems, equipment, and applications that are the subject of the agreement or their technical characteristics.
- V. With respect to the Technological Infrastructure and information security, in addition to the information determined in these Provisions, Article 49, part III, paragraphs b) and d), the following documentation must be available:
 - a) Description of the technical characteristics of the systems, equipment, and applications that are the subject of the agreement.
 - b) The one detailing the mechanisms to ensure the transmission and storage of Personal Information or Sensitive Information in Encrypted form, if applicable, including the version of the Encryption protocols and security components in the Technological Infrastructure.

In the case of Sensitive Information, the data related to Transactions is exempted from Encryption, provided that such data is stored in tables or archives different from those used to store the rest of the Personal Information and Sensitive Information and that security mechanisms are in place to prevent the integration of such separate archives if not authorized to do so.

- c) The one that contains the detail of the type of information of the electronic payment funds institution and Client specifying, as the case may be, the type of Personal Information or Sensitive Information that will be stored by the third party in its equipment or facilities, or to which it may have access.
 - d) The description of the mechanisms for controlling and monitoring access to the computer systems and to the Personal Information or Sensitive Information transmitted, stored, processed, safeguarded, or guarded in such systems, as well as the logs, databases, and security configurations established for such purpose.
 - e) Evidence of the controls and control mechanisms referred to in these Provisions, Article 49, part V.
- VI. Have the evidence referred to in these Provisions, Article 49, part VIII.

Article 52.- The electronic payment funds institutions must have a list of all the service providers, including those providers subcontracted by them, as well as the Commission Manager

and contracted commission agents, containing at least the following information:

I. Service providers:

- a) Name, or corporate name of the service provider.
- b) Name of the legal representative of the service provider.
- c) Description of the service contracted with the third party, including the data or information, if any, that is stored, processed, or transmitted by the third party.
- d) If applicable, information on the systems that support the service contracted with the third party, including, at least, the name, version and function or purpose.
- e) If applicable, interfaces with other systems and the purpose of these, including details of the information exchanged.
- f) The location where the service is performed and where the personnel responsible for carrying it out is located.
- g) If applicable, the location or jurisdiction of the main data center where the processing equipment of the contracted system is located.
- h) If applicable, the location or jurisdiction of the alternate data center where the processing equipment is located, in the case of recovering the contracted service.
- i) If applicable, the number and date of the official notice with which Banco de México and the National Banking and Securities Commission (CNBV) granted the authorization to act as a service provider.

II. Administrator of Commission Agents or commission agents:

- a) Name, denomination, or name of the corporation of the commission agent or the Administrator of Commission Agents.
- b) Name of the legal representative of the commission agent or the Administrator of Commission Agents.
- c) Trade name of the commission agent or Administrator of Commission Agents, as well as details of the commercial modality under which it operates, whether it is a commercial chain or franchise.
- d) Number of establishments of the commission agent in which the agency commissions are carried out, and for each one of them, its complete address, including the code of the geostatistical locality in accordance with the Unified Catalog of Codes of State, Municipal and Local Geostatistical Areas of the National Institute of Statistics and Geography, or the one that replaces it.
- e) Type of operation carried out by the commission agent on behalf of and for the account of the electronic payment funds institution.
- f) Limits of the Transactions agreed with the commission agent or with the

Administrator of Commission Agents.

- g) Access devices used to offer services to Clients, such as cell phones, tablets, and point-of-sale terminals, among others.
- h) If applicable, the number of the legal paper and the date on which the authorization was granted for the hiring of the commission agent or Administrator of Commission Agents.

The electronic payment funds institutions must disseminate through their website or application the list of the modules or establishments that the commission agents or the Administrator of Commission Agents have authorized to carry out the Transactions referred to in these Provisions, Article 47, specifying the Transactions that may be carried out in each one of them and the maximum amounts authorized per Operation.

The electronic payment funds institutions must keep the registry referred to in this article up to date.

Article 53.- The electronic payment funds institution must perform, at least annually, by itself or through a third party, audits aimed at verifying the degree of compliance with these Provisions. If the commission agent or Administrator of Commission Agents has the results of an audit previously carried out for the same purpose, with a maximum validity of one (1) year, they may submit them to the electronic payment funds institution. Notwithstanding the foregoing, the National Banking and Securities Commission, (CNBV) may order the performance of audits when, in its judgment, there are risk conditions in terms of operation and information security.

Article 54.- At all times, the electronic payment funds institutions must keep fully identified the Transactions carried out through the commission agent or the Administrator of Commission Agents, independently from those carried out through their platforms.

Likewise, the electronic payment funds institutions must verify that the commission agents or Administrator of Commission Agents inform the Clients of the institutions themselves by any means that they act in the name and on behalf of the institution in question.

Article 55.- The electronic payment funds institutions must be liable at all times, both for the service that their commission agents or Administrator of Commission Agents provide to the Clients, even when the execution of the corresponding Transactions is carried out under terms different from those agreed upon, as well as for the non-compliance with the provisions incurred by such commission agents.

In case of non-compliance by the commission agents or Administrator of Commission Agents with the applicable provisions, the electronic payment funds institutions must implement the necessary corrective measures.

The provisions of the two preceding paragraphs must be without prejudice to the civil, administrative, or criminal liabilities that the commission agents, the Administrator of Commission Agents, or their employees may incur due to violations of the applicable legal provisions.

The provisions of the preceding paragraph must be set forth in the agreement, which is made and entered into by and between the electronic payment funds institution and the commission agent or the Administrator of Commission Agents.

CHAPTER VI

Independent third-party evaluation

article 56. - The electronic payment funds institutions must contract the services of an Independent Third Party or of the legal entity through which said Independent Third Party renders its services to perform the evaluation of the level of compliance with the information security requirements, the use of Instruction Channels and the operational continuity that said institutions must observe in accordance with these Provisions, Chapters II, III, IV, and V.

Article 57.- The evaluation of the level of compliance performed by the Independent Third Party referred to in the preceding article must be carried out every two years.

The compliance evaluation report must be submitted by the Independent Third Party to the Management Body of the electronic payment funds institution and presented to the audit committee of such institution when available.

Electronic payment funds institutions may not contract the services of an Independent Third Party, or of the legal entities through which they provide the respective services, to obtain the compliance evaluation referred to in this article for more than two consecutive evaluation periods. Notwithstanding the foregoing, the electronic payment funds institution may designate again the same Independent Third Party or legal entity referred to, after a minimum interruption of five (5) years from the last compliance evaluation it has granted with respect to such institution.

If the evaluation carried out results in observations which, in the opinion of the Independent Third Party, represent serious violations, the electronic payment funds institution in question must submit the compliance evaluation report to its Board of Directors within twenty (20) business days following the end of the evaluation by the Independent Third Party, or within five (5) business days in the case of a Sole Administrator.

The report indicated in the preceding paragraph must be delivered to Banco de México and the National Banking and Securities Commission (CNBV), following these Provisions, Article 59, within five (5) business days from the day following the day on which such report is submitted to its Management Body. The CEO must digitally sign the report or, as the case may be, the sole administrator and encrypt it following the provisions of Article 59.

In addition, the electronic payment funds institution must submit, in accordance with these Provisions, Article 59, and within twenty (20) business days following the completion of the evaluation conducted by the Independent Third Party, a remediation plan to remedy such observations. The CEO must digitally sign the remediation plan or, as the case may be, the sole administrator and encrypted following the provisions of the aforementioned Article 59. The National Banking and Securities Commission (CNBV) and Banco de México may comment on the remediation plan anytime.

Article 58. - The Independent Third Parties that evaluate the level of compliance of the electronic payment funds institutions with the rules contained in these Provisions, as well as the legal entities through which they render the respective services, must be independent as of

the date of execution of the agreement for rendering services, during the development of the compliance evaluation and until the issuance of the compliance evaluation report in question, and must comply with these Provisions, Annex 6.

CHAPTER VII

Supplementary provisions

Article 59. - In the case of documents containing requests, reports, reports and work or remediation plans that electronic payment funds institutions must submit through the website that the National Banking and Securities Commission (CNBV) and Banco de México make available to such institutions at the time they obtain authorization to organize themselves as such, for the purposes set forth in these Provisions, Articles 6, 11, 26, 26, 33, 34, 43, 44, 45, 46 and 57, they must be submitted with the respective electronic signatures of the corresponding representatives and, in the cases indicated, be encrypted in accordance with the following:

- I. Use of cryptographic keys, known as asymmetric public and private keys, for each electronic signature, in order to guarantee confidentiality and non-repudiation, avoiding the sharing of the private key.
- II. Use of a digital certificate validated by a recognized certification agency, or a certification service provider accredited by the Ministry of Economy.
- III. Incorporation of electronic signature to guarantee the integrity of the information provided.

The information of the public cryptographic keys to encrypt the data message that constitutes the respective document must be published on the website that the Financial Authorities referred to in the first paragraph of this article must make available to the electronic payment funds institutions. To perform the encryption, such institutions may use the information system of Banco de México called “WebSec” or any other system developed by a third party that complies with the Provisions, Annex 8.

In those cases in which the website referred to in this article in the first paragraph is not available or the electronic payment funds institutions do not have the necessary elements to be able to use electronic signatures in the documents referred to in this article, the referred institutions must submit such documents through the Electronic Attention Module, known as MAE, of Banco de México, in terms of the applicable provisions issued by Banco de México itself for such purposes, or in the absence of such module, by the means provided by Banco de México.

The resolutions issued with respect to the documentation entered into the Internet site of the aforementioned Financial Authorities, in accordance with the provisions of this article, must be delivered jointly by said authorities, through the aforementioned Internet site.

Transitory provisions

ONE. - These Provisions must become effective ninety (90) calendar days following their publication in the Federal Official Gazette.

TWO. - The electronic payment funds institutions must have a maximum term of six (6) months, counted as these Provisions become effective, to comply with these Provisions, Article 15.

THREE. - The electronic payment funds institutions must have a term of nine (9) months, counted as these Provisions come effective, to comply with the herein Provisions, Articles 16 and 17.

FOUR. The persons referred to in the 8th Transitory Provision of the Fintech Law published in the Official Gazette on March 9, 2018, will have a term of six (6) months counted from the date of obtaining their authorization to act as an electronic payment funds institution, to comply with the established on these Provisions, Articles 44, 45, 46 and 47.

Mexico City, January 15, 2021.- BANCO DE MEXICO: General Director of the Payment Systems and Market Infrastructures, **Manuel Miguel Ángel Díaz Díaz** Signature. - General Counsel, **Luis Urrutia Corral**.- Signature.- NATIONAL BANKING AND SECURITIES COMMISSION: Chairperson **Juan Pablo Graf Noriega**.- Signature.

ANNEX 1 Information Security Indicators

The chief information security officer of the electronic payment funds institution, about the information security risk indicators referred to Provisions, Article 36, Section XI, must:

1. Evaluate these indicators, which must comply with the thresholds contained in this annex for each indicator. If different thresholds are defined, the reason must be documented.
2. Define remediation plans for those risks in which the results of the evaluation show values within the medium and high-risk thresholds established in this Annex or, as the case may be, those defined by the electronic payment funds institution, provided that they are in a high threshold for at least two consecutive periods.
3. Provide ongoing maintenance, either to add, eliminate or update the existing information security key risk and performance indicators, which must always be aligned with the strategy of the electronic payment funds institution and the Information Security Master Plan of the Institution.
4. Measure and evaluate its evolution with the periodicity indicated in the following tables, or earlier in case of unusual events.
5. If not, all assumptions apply, indicate that they do not apply and explain the reason.

Type	Definition	Subtype	Subclass of Events	Examples
I. Internal Fraud	Losses arising from any action to defraud, misappropriate assets, or otherwise avoid regulations, laws, or corporate policies (not including diversity events / discrimination) in which at least one party internal to the Electronic Payment Funds Institution is involved.	1.1 Unauthorized Activities.	1.1.1 Misuse of powers and authority 1.1.2 Transactions not disclosed (intentionally). 1.1.3 Unauthorized Transactions (with pecuniary losses). 1.1.4 Erroneous valuation of positions (intentional).	Unreported Transactions; unauthorized operations (with pecuniary losses); erroneous valuation of positions; and intentional omission of regulations.
		1.2 Internal Robbery and Fraud.	1.2.1 Fraud / credit fraud / worthless deposits. 1.2.2 Theft / Extortion / Embezzlement / Robbery. 1.2.3 Misappropriation of assets. 1.2.4 Fraudulent destruction of assets. 1.2.5 Internal Forgery. 1.2.6 Smuggling 1.2.7 Appropriation of accounts, identity, among others. 1.2.8 Non-compliance / tax evasion (intentional) 1.2.9 Bribery. 1.2.10 Insider trading (not in favor of the company).	Robbery, embezzlement, misappropriation, destruction of assets, forgery, impersonation, bribery, manipulation of accounts.
		1.3. Vulnerability to system security.	1.3.1 Vulnerability of security systems. 1.3.2 Damage due to computer attacks. 1.3.3 Data theft (with pecuniary losses). 1.3.4 Inappropriate use of passwords and/or authorization levels.	Abuse and use of privileged or confidential information; alteration of computer applications; theft of passwords; and prohibited computer access.
		1.4 Identity Theft	1.4.1 Internal forgery / impersonation	Internal forgery and impersonation
II. External Fraud	Losses derived from any action aimed at defrauding, misappropriating assets, or circumventing the law by a third party.	2.1 External Fraud.	2.1.1 Use and/or disclosure of privileged information. 2.1.2 Industrial Espionage. 2.1.3 Smuggling.	Misuse of stolen, counterfeit, stolen or blacklisted cards.
		2.2 Systems Security.	2.2.1 Vulnerability of security systems. 2.2.2 Damage due to computer attacks. 2.2.3 Data theft (with pecuniary losses). 2.2.4 Inappropriate use of passwords and/or authorization levels.	Unauthorized computer access, manipulation of computer applications, damage due to computer attacks, and information theft.
		2.4 Identity theft	2.4.1 External forgery / Impersonation	Forged Documents or manipulated (transfers, etc.); identity theft.
VI. Business Incidents and System Failures	Losses derived from business incidents and system failures.	6.1 Systems	6.1.1 Hardware. 6.1.2 Software. 6.1.3 Telecommunications. 6.1.4 Interruption / Supply incidents.	Interruption/incidents in supplies and communication lines; errors in computer programs; hardware and software failures; sabotage; business interruptions; computer failures; and virus programming.

ID	Name	Description	Domain	Type	Subtype	Subclass of Events	Type Indicator	Period	Measure of Unit	Calculation	Variable X	Variable Y	High Risk	Medium Risk	Low Risk
KR0001	Incidents through direct attacks against internal systems.	Number of incidents that attacks on the internal systems of the electronic payment funds institution in the established period have originated.	Logical attacks.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	Reactive.	Quarterly.	Quantity.	Variable X	Number of cases of identified incidents.	-	More than 1.	Equal to 1.	Equal to 0.
KR0002	Cases of fraud on the platform.	Percentage of cases where fraud is identified as having originated from attacks on the Platform.	Logical attacks.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	Reactive.	Monthly.	Percentage.	$(XY) \cdot 100$	Number of fraud cases in the Platform.	Number of Clients using the Platform.	More than .01%.	Between 0.005% and 0.01%.	More than 95%.
KR0003	Technological Infrastructure equipment whose security configuration is managed.	Percentage of Technological Infrastructure equipment within the Platform and/or secure configuration standards review process concerning the total Electronic Payment Funds Institution (EPFI) equipment during the established period.	Compliance.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	Preventive.	Monthly.	Percentage.	$(XY) \cdot 100$	Number of teams within the platform to secure configuration standards review process.	Total number of teams.	Less than 85%.	Between 85% and 95%.	More than 95%.
KR0004	Level compliance with secure configuration servers whose configuration is managed.	Average percentage of compliance level of servers covered by the secure configuration standards review tool and/or process.	Compliance.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	Preventive.	Monthly.	Percentage average.	Average(X)	% of compliance with the secure configuration standard of each of the Servers.	-	Less than 90%.	Between 90% and 95%.	More than 95%.
KR0005	Users with inadequate roles and profiles.	Percentage of users with inadequate profiles within the company. Applications of the EPFIs, with respect to the total number of users in all of the applications of the Electronic Payment Funds Institution.	Compliance.	I. Internal Fraud.	1.3. Security systems.	1.3.3 Data theft (with pecuniary losses). 1.3.4. Inappropriate use of passwords and/or authorization levels.	Corrective.	Semi annual.	Percentage.	$(XY) \cdot 100$	Number users with incorrect profiles, considering all applications.	Total number of users considering all applications	More than 3%.	Between 1% and 3%.	Less than 1%.
KR0006	Role and profile applications.	Percentage of applications which do not have the ability to nor role profiling and permits, or that such roles and are not implemented, this with regarding the total of applications.	Compliance.	I. Internal Fraud.	1.3. Security systems.	1.3.3 Data theft (with pecuniary losses).	Corrective.	Quarterly.	Percentage.	$(XY) \cdot 100$	Number of applications not built	Total number of applications	More than 5%.	Between 2% and 5%.	Less than 2%.
KR0007	General information of the security incidents	Total number of incidents reported during the reporting period related to information security.	Information.	Applies to: I. Internal Fraud II. External Fraud VI. Incidents in the Business and Systems Failures.	Applicable to: 1.3. Security systems 2.2 Systems Security. 6.1 Systems.	Applicable to: 1.3.1 Vulnerability of security systems 1.3.2 Damage due to computer attacks. 1.3.3 Data theft (with pecuniary losses). 1.3.4 Inappropriate use of passwords and/or authorization levels. 2.2.1 Vulnerability of security systems. 2.2.2 Damage due to computer attacks. 2.2.3 Data theft (with pecuniary losses). 2.2.4 Inappropriate use of passwords and/or authorization levels. 6.1.1 Hardware. 6.1.2 Software.	Reactive.	Monthly.	Quantity.	Variable X.	Security incident number of information	-	More than 5.	From 2 to 5.	Less than 2.

6.1.3 Telecommunications.

6.1.4 Interruption of Supply									
Platform technological obsolete and/or outdated	Infrastructure.	II. Fraud External.	2.2 Safety of Systems.	2.2.1 Vulnerability Security Systems.	of Corrective Action.	Semi annual	Percentage.	(XV) *10.	Number of platforms technological obsolete.
Percentage technological platforms that are located on obsolete versions and/or without the support of the manufacturer	Infrastructure.	II. Fraud External.	2.2 Safety of Systems.	2.2.1 Vulnerability Security Systems.	of Corrective Action.	Semi annual	Percentage.	(XV) *10.	Number of platforms technological obsolete.
Number of systems related to the services provided to their Clients.	Infrastructure.	VI. Incidents in the Business and Failures in system	6.1 Systems.	6.1.4 Interruption /	Reactive.	Monthly.	Quantity.	Variable X.	Number of falls of systems.
Incidents by vulnerabilities provided by providers (third parties)	Infrastructure.	II. Fraud External.	2.2 Safety of Systems.	2.2.1 Vulnerability Security Systems.	of Preventive.	Monthly.	Percentage.	(XV) *100.	Number of incidents attributed to vulnerabilities in systems provided by providers
Critical vulnerabilities to be addressed correct the evidence of ethical hacking tests.	Infrastructure.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	of Preventive.	Monthly.	Quantity.	Variable X.	Number of critical vulnerabilities pending correction that are more than one month old.
Unavailability of IT systems.	Infrastructure.	VI. Incidents in the Business and Systems Failures.	6.1 Systems.	6.1.4 Interruption of incidents in the Supply.	/ Reactive, the	Monthly.	Percentage Average.	Average(X).	Average time Unavailability of IT systems.
Critical and high priority incidents in production environments.	Infrastructure.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	of Reactive.	Monthly.	Percentage.	(XV) *100.	Number of qualified critical production incidents.
Technological vulnerabilities exposed to the Internet without evidence of ethical hacking and/or analysis of vulnerabilities.	Infrastructure.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	of Corrective Action.	Quarterly.	Percentage.	(XV) *100.	Number of assets exposed to the Internet. Number of ethical hacking tests or vulnerability analysis.
Vulnerabilities in the information systems that, according to the analysis of	Infrastructure.	II. Fraud External.	2.2 Safety of Systems.	2.2.1 Vulnerability Security Systems.	of Corrective Action.	Monthly.	Quantity.	Variable X.	Number total vulnerabilities critical.
Vulnerabilities are catalogued as critical, which have more than one month of seniority to as of its date of detection.									


KR0016	Obsolete and/or unsupported Technological Infrastructure.	Number of equipment and Technological Infrastructure which are in obsolete or unsupported versions, compared to the entire IT infrastructure active in the established period.	Infrastructure.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	Corrective.	Quarterly.	Percentage.	(XV) *100.	Number of obsolete equipment and infrastructure.	Total number of active teams.	More than 5%.	Between 2% and 5%.	Less than 2%.
KR0017	Servers <i>antimauware</i> solution.	Percentage of servers without <i>antimauware</i> in relation to the total number of servers.	Malware.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	Corrective.	Monthly.	Percentage.	(XV) *100.	Number of servers without <i>antimauware</i> .	Total number of servers.	More than 6%.	Between 3% and 6%.	Less than 3%.
KR0018	Servers signatures of outdated <i>antimauware</i> or outdated.	Percentage of servers with signatures of outdated <i>antimauware</i> (concerning the total number of servers with <i>antimauware</i> in each Electronic Payment Funds Institution (EPTI).	Malware.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	Corrective.	Monthly.	Percentage.	(XV) *100.	Number of servers with outdated <i>antimauware</i> signatures.	Total number of servers with <i>antimauware</i> .	More than 6%.	Between 3% and 6%.	Less than 3%.
KR0019	Workstations without <i>antimauware</i> solution	Percentage of workstations without <i>antimauware</i> with respect to the total of equipment	Malware.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	Corrective.	Monthly.	Percentage.	(XV) *100.	Number of workstations without <i>antimauware</i> .	Total number of workstations.	More than 8%.	Between 4% and 8%.	Less than 4%.
KR0020	Workstations with signatures of outdated <i>antimauware</i> or outdated.	Percentage of workstations with signatures of outdated <i>antimauware</i> (concerning the total number of computers with <i>antimauware</i> installed.	Malware.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	Corrective.	Monthly.	Percentage.	(XV) *100.	Number of workstations with outdated <i>antimauware</i> signatures.	Number of workstations with <i>antimauware</i> .	More than 8%.	Between 4% and 8%.	Less than 4%.
KR0021	Incidents of security features attributed to personnel providers (third parties) that do not belong to the Electronic Payment Funds Institution (EPTI), payroll, reported during the established period, concerning the total number of security incidents.	Percentage of incidents related to personnel providers (third parties) that do not belong to the Electronic Payment Funds Institution (EPTI), payroll, reported during the established period, concerning the total number of security incidents.	Incidents.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	Reactive.	Monthly.	Percentage.	(XV) *100.	Number of incidents of security related with personnel providers (third parties).	Number of total security incidents of providers (third parties).	More than 5%.	Greater than 0 % and less than 5 %.	Equal to 0 %.
KR0022	Servers with versions of obsolete operating systems.	Total percentage of servers with obsolete operating systems version compared to total number of servers.	Software.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	Corrective.	Monthly.	Percentage.	(XV) *100.	Number of servers with system operationally obsolete.	Total number of servers.	More than 10%.	Between 5% and 10%.	Less than 5%.
KR0023	Applications in production with partial or deficient compliance with security controls.	Percentage of applications in production with partial or deficient compliance, with respect to the policies of security established, in security issues, with respect to the total number of applications.	Software.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	Corrective.	Quarterly.	Percentage.	(XV) *100.	Number of deficient security controls in production applications.	Total number of security controls.	More than 5%.	Between 2% and 5%.	Less than 2%.
KR0024	Data base managers (DBM) with versions of obsolete or unsupported technology.	Percentage of data base managers (DBM), which are versions of obsolete technologies or not supported by the manufacturer, compared to the total number of data base managers (DBM) active in the established period.	Software.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	Corrective.	Quarterly.	Percentage.	(XV) *100.	Number of database managers (DBM) obsolete or not supported.	Total number of data base managers (DBM).	More than 10 %.	Between 5 % and 10 %.	Less than 5%.
KR0025	Obsolete or unsupported applications.	Percentage of applications within the EPTI, which are obsolete or unsupported by the manufacturer, in relation to all active applications during the established period.	Software.	II. External Fraud.	2.2 Systems Security.	2.2.1 Vulnerability of security systems.	Corrective.	Quarterly.	Percentage.	(XV) *100.	Number of obsolete or unsupported applications.	Total active applications.	More than 5%.	Between 2% and 5%.	Less than 2%.

KR0026	Servers without coverage security patches.	Percentage of servers without the latest security patches, with respect to the total number of servers active during the established period.	Software.	II. External Fraud.	2.2 Systems Security.	2.2.1 Violation of security systems.	Corrective.	Monthly.	Percentage.	(XV) *100.	Number of servers without the latest security patches installed.	Total of servers.	More than 5%.	Between 2% and 5%.	Less than 2%.
KR0027	Workstations without coverage security patches	Percentage of workstations without the most recent security patches, regardless of the operating system at issue, with respect to the total number of workstations of EPEIs.	Software.	II. External Fraud.	2.2 Systems Security.	2.2.1 Violation of security systems.	Corrective.	Monthly.	Percentage.	(XV) *100.	Total number of workstations without the latest security patches installed.	Number of total workstations.	More than 3%.	Between 1 % and 3 %.	Less than 1%.
KR0028	Data base managers (DBM) without security patch coverage.	Percentage of database managers (DBMs) without coverage of the most recent security patches, with respect to the total number of database managers (DBMs) during the established period.	Software.	II. External Fraud.	2.2 Systems Security.	2.2.1 Violation of security systems.	Preventive.	Quarterly.	Percentage.	(XV) *100.	Number of database managers (DBM) without security patch coverage.	Total number of database managers (DBM).	More than 5%.	Between 2% and 5%.	Less than 2%.

Minimum requirements to develop a Business Continuity Plan

The electronic payment funds institutions, prior to the development of the Business Continuity Plan, must carry out the following:

- I. A risk analysis that:
 - a) deems risks associated with the following factors: human (including fraud, integrity, training), process, technological, and external (including external suppliers) in accordance with the methodology referred to in these Provisions, Article 39.
 - b) identifies, evaluates, monitors, and mitigates risks related to operational processes and data processing and transmission services contracted with suppliers, as well as those related to custody and safekeeping of information of the electronic payment funds institution and its Clients.
 - c) Determine the risks derived from the geographic location of the primary data processing and operation centers of the processes identified as critical according to the business impact analysis to prevent alternate data processing and operation centers from being exposed simultaneously to the same risks as the main ones.
 - d) Evaluate the need to establish alternate sites or services for information processing and operation, which, if applicable, must be able to operate when required and not be subject at the same time to the same risks as the primary site.
- II. A business impact analysis that:
 - a) Contains the totality of services and processes, identifying those that are critical and considered indispensable for the continuity of operations, including the services contracted with its service providers.
 - b) Determines the minimum human, logistical, material, Technological Infrastructure, and any other type of resources necessary to maintain and reestablish the services and processes of the electronic payment funds institution in the event of an Operational Contingency and upon its termination.
 - c) Elaborate relevant scenarios related to possible Operational Contingencies, considering, among others, the following:
 1. Natural and environmental disasters.
 2. Infectious diseases.
 3. Cyberattacks or attacks on computer activity.
 4. Sabotage.
 5. Terrorism.

- 
- 6. Power supply interruptions.
 - 7. Failures or unavailability of the Technological Infrastructure.
 - 8. Unavailability of human, material, or technical resources.
 - 9. Interruptions in services provided by third parties.
- d) Estimate the quantitative and qualitative impacts of the Operational Contingencies based on the scenarios defined for each process and through the methodologies referred to in these Provisions, Article 39.
 - e) Defines the recovery priority for each of the processes.
 - f) Determines the recovery time objective (RTO) for each of the services and processes. In the case of processes considered as critical, the recovery time does not exceed two hours.
 - g) Establishes the recovery point objective (known as RPO), understood as the maximum tolerable data loss for each of the services and processes, considering that the information of those operations already performed cannot be lost in any scenario and that the status of each operation held at the time of the Operational Contingency is known, on time.
 - h) Identifies and evaluates the risks related to operational processes and data processing and transmission services contracted with suppliers, as well as the risks associated with the custody and safekeeping of the information of the electronic payment funds institution.
- III. The Business Continuity Plan must indicate the processes that must be prioritized for recovery when an Operational Contingency occurs, in accordance with the impact analysis referred to in this Annex, part II.
- IV. In the development of the Business Continuity Plan, at least the following actions must be incorporated:
- a) Prevention, which must include, at least, the determination of the activities and procedures related to:
 - 1. The reduction of vulnerabilities in the processes and services of the electronic payment funds institution in the face of Operational Contingencies.
 - 2. The availability of the human, financial, material, technical, and Technological Infrastructure resources necessary to act in a timely manner in the event of an Operational Contingency.
 - 3. The establishment of an annual testing program, or earlier if there is a meaningful change in the Technological Infrastructure, processes, products,

and services, or internal organization of the institution, regarding the operation and adequacy of the Business Continuity Plan that evaluates all its stages and components.

4. Policies and procedures for training personnel involved in the processes and developing the plan.
 5. Procedures for registration, attention, follow-up, and dissemination to personnel whose functions are affected by the Operational Contingency or related to the execution of the Business Continuity Plan of the findings, incidents, or observations resulting from the tests on the operation and sufficiency of such plan, or the execution of the same in the event of an Operational Contingency having occurred.
- b) Contingency, which must include the definition of authorized response actions and procedures for:
1. Identifying in a timely manner the nature of the Operational Contingencies that affect the critical processes of the electronic payment funds institution.
 2. Containing the effects of operational contingencies on critical processes and favoring the reestablishment of the operation to the required operating levels.
 3. Informing Banco de México and the CNBV of the Operating Contingencies, in accordance with these Provisions, Article 43.
- c) Recovery, which must include the definition of the actions and procedures to be followed so that the services and processes of the electronic payment funds institutions, in the event of the materialization of Operational Contingencies, may continue their operation at a minimum acceptable level, including mechanisms for updating and reconciliation of information, as well as the mechanisms for recovery in the event of updating these Provisions, Article 49, part VII.
- d) Restoration must include the definition of the actions and procedures for the services and processes of the electronic payment funds institutions to return to regular operation after the execution of the recovery actions due to the occurrence of any Operational Contingency.
- e) Evaluation, which must include the collection and analysis of relevant information on the development of the Operational Contingency and the actions and procedures followed for its prevention, containment, recovery, and restoration to, if necessary, make the adjustments required for the Business Continuity Plan.

When defining the different actions and procedures referred to in this part, the electronic payment funds institutions must, at all times, precisely determine the responsible personnel, as well as provide for their substitution or replacement if the holders are not present or available to carry out what the Business Continuity Plan establishes.

ANNEX 3

Information Security Incidents

- I. Information on the electronic payment funds institution
 - a) Name of the electronic payment funds institution
 - b) The full name of the chief information security officer and their telephone number and e-mail address.
- II. Detailed Information of the Information Security Incident

Description of the Information Security Incident		
a) Date and time of occurrence		
b) Date and time of detection		
c) Duration of the incident		
d) Is the information involved in the incident managed by third parties?	Yes ()	No ()
e) If d) is affirmative, please provide details of the supplier (name, address, contact information, e-mail, telephone, among others).		

Impact of the Information Security Incident		
f) Is the incident likely to result in a monetary loss to Clients or the EPFI itself?	Yes ()	No ()
g) Is it feasible to recover the possible monetary loss directly (through own procedures) or indirectly (through insurance)?	Yes ()	No ()
h) Have other incidents related to the one reported been identified, either by origin, mode of operation, or impact?	Yes ()	No ()

i) Indicate, if applicable, the type of information compromised by the Information Security Incident, according to the following tables:

Compromised Client Personal Information		
Names	Yes ()	No ()
Domiciles	Yes ()	No ()
Telephone numbers	Yes ()	No ()
E-mail addresses	Yes ()	No ()
Biometric data (fingerprints, iris, or retina patterns, facial recognition, etc.)	Yes ()	No ()
Other(s):		

Account or balance information		
Card numbers, or other	Yes ()	No ()
Account Numbers	Yes ()	No ()
Passwords or Client Identifier numbers	Yes ()	No ()
Client Identifiers	Yes ()	No ()
Limits	Yes ()	No ()
Balances	Yes ()	No ()
Other(s)		

Information on the electronic payment funds institution		
Passwords	Yes ()	No ()
Security settings	Yes ()	No ()
Identification of ports or services	Yes ()	No ()
IP addresses of components or services	Yes ()	No ()
IP addresses of internal components	Yes ()	No ()
Access to internal network segments	Yes ()	No ()
Versions of software, operating systems, or databases	Yes ()	No ()
Vulnerability identification	Yes ()	No ()
Other(s)		

III. Classify the reported Information Security Incident based on the following definitions:

a) Unintentional or accidental damage, loss of information, or loss of assets		
Improperly shared information	Yes ()	No ()
Errors or omissions in systems or devices	Yes ()	No ()
Errors in procedures or controls	Yes ()	No ()
Improper changes to data	Yes ()	No ()
Loss of information or devices	Yes ()	No ()
Other(s):		
b) Incidents due to failures or malfunctions		
Devices	Yes ()	No ()
Systems	Yes ()	No ()
Communications	Yes ()	No ()
Services	Yes ()	No ()
Third-party equipment	Yes ()	No ()

Supply chain	Yes ()	No ()
Other(s):		
c) Incidents due to interruption or lack of inputs		
Absence of personnel	Yes ()	No ()
Strikes	Yes ()	No ()
Energy	Yes ()	No ()
Water	Yes ()	No ()
Telecommunications	Yes ()	No ()
Other(s):		
d) Data interception incidents		
Espionage	Yes ()	No ()
Messages	Yes ()	No ()
<i>Wardriving</i>	Yes ()	No ()
Man-in-the-middle attacks	Yes ()	No ()

Session hijacking	Yes ()	No ()
<i>Sniffers</i>	Yes ()	No ()
Courier theft	Yes ()	No ()
Other(s):		
e) Incidents due to malicious activity with the purpose of taking control of, destabilizing, or damaging a computer system.		
Identity Theft	Yes ()	No ()
<i>Phishing</i>	Yes ()	No ()
Denial of services (DOS, DDOS)	Yes ()	No ()
Malicious code (<i>malware</i> , trojans, worms, code injection, viruses, <i>ransomware</i>)	Yes ()	No ()
Social engineering	Yes ()	No ()
Certificate violation (site spoofing, fake certificates)	Yes ()	No ()
Hardware manipulation (<i>proxies</i> anonymous, <i>skimmers</i> , <i>sniffers</i>)	Yes ()	No ()
Alteration of information (spoofing of addressing and routing tables, DNS, etc.) <i>poisoning</i> , alteration of configurations)	Yes ()	No ()
Abuse of auditing applications	Yes ()	No ()
Brute force attacks	Yes ()	No ()

Abuse of authorizations	Yes ()	No ()
Organized crime	Yes ()	No ()
Hacktivists	Yes ()	No ()
Government or related groups	Yes ()	No ()
Terrorists	Yes ()	No ()
<i>Insiders</i>	Yes ()	No ()
Other(s):		
f) Incidents arising from legal issues		
Violation of contractual clauses	Yes ()	No ()
Breach of confidentiality agreements	Yes ()	No ()
Adverse decisions (court rulings in the same or other jurisdictions)	Yes ()	No ()
Other(s):		
g) Other (specify)		

IV. Classification of the Information Security Incident

Indicate in the following table the classification in which the incident is located by means of the items in the catalog indicated below:

Type	Subtype	Subclass of Events	
I. Internal Fraud	Unauthorized Activities.	Transactions not disclosed (intentionally).	()
		Unauthorized Transactions (with pecuniary losses).	()
		Erroneous valuation of positions (intentional).	()
	1.2 Internal Robbery and Fraud.	Fraud / worthless deposits.	()
		Extortion/embezzlement/theft.	()
		Misappropriation of assets.	()
		Fraudulent destruction of assets.	()
		Internal Forgery.	()
		Smuggling.	()
		Appropriation of accounts, identity, among others.	()
		Noncompliance / tax evasion . (intentional).	()
		Bribery.	()
		Insider trading (not in favor of the company).	()
	1.3. System security.	Vulnerability of security systems.	()
		Damage due to computer attacks.	()
		Data theft (with pecuniary losses).	()
		Inappropriate use of passwords and/or authorization levels.	()
			()

II. External Fraud	External Theft and Robbery / swindling / extortion / bribery.	()
	Fraud.	
	External Forgery/ Personality	()
	Impersonation	()
	Use and/or disclosure of privileged information.	()
	Industrial Espionage.	()
	Smuggling.	
	2.2 Systems Security.	Vulnerability of security systems. ()
		Damage due to computer attacks. ()
		Data theft (with pecuniary losses). ()
		Inappropriate use of passwords and/or authorization levels. ()
VI. Business Incidents and System Failures	Systems	Hardware. ()
		Software. ()
		Telecommunications. ()
		Interruption / Supply incidents. ()

Name and signature of chief information security officer

ANNEX 4

Information Security Incident Report

- I.** Information on the electronic payment funds institution
 - a)** Name of the electronic payment funds institution
 - b)** Full name of the information security officer, as well as his or her telephone number and e-mail address.
- II.** Detailed Information of the Information Security Incident
 - a)** Attach, in encrypted digital media, the following information:
 - 1.** Description of the Information Security Incident.
 - 2.** Affected account numbers.
 - 3.** Status of affected accounts (blocked, suspended, active).
 - 4.** Affected network area (Internet, internal network, administration network, among others).
 - 5.** Type of affected system (file server, web server, mail service, database, workstations, whether desktop or mobile, among others).
 - 6.** Operating system (specify version).
 - 7.** Protocols or services of the impacted components.
 - 8.** Number of components of the affected systems of the electronic payment funds institution.
 - 9.** Involved applications (specify version).
 - 10.** Compromised device information, if applicable (brand, software version, etc.), *firmware*, among others).
 - 11.** Impact on the service (considering any disruption) caused by the Information Security Incident.
 - 12.** Amount of loss in pesos, if any.
 - 13.** Amount recovered in pesos, if applicable.
 - 14.** Information Security Incident Status (Resolved or Not Resolved).
 - 15.** Indicate whether the Information Security Incident has been reported to any authority. If yes, indicate the authority and date.
 - 16.** Public IP addresses, email addresses, or domains from which the attack

originates.

- 17.** The communication protocol used, if any.
- 18.** The URL in case of websites involved.
- 19.** The malware or signature detected.
- 20.** Detail the actions taken to mitigate the Information Security Incident, mentioning the persons responsible for implementing such mitigation actions.
- 21.** Description of the results of the mitigation actions.
- 22.** Incident recovery times.
- 23.** Actions to minimize damage in subsequent similar situations.
- 24.** Other information that the National Banking and Securities Commission must be aware of.
- 25.** Communication actions with Clients to inform them of the incident.

Name and signature of chief information security officer

ANNEX 5

Report on Operational Contingencies

- I. Information on the electronic payment funds institution
 - a) Name of the electronic payment funds institution
 - b) Author of the report.
 - c) Position/area
 - d) Email
 - e) Telephone number
- II. Detailed information on the Operational Contingency

Description of the Operational Contingency	
a) Date and time of occurrence	
b) Date and time of detection	
c) Duration of operational contingency	
d) Location(s) of affected facility(ies) (data center, offices)	
e) Failures or malfunctions in the Technological Infrastructure that supports the services.	Yes () No ()
g) Affection in the critical components of the Technological Infrastructure that has had as a consequence the total or partial activation of the Business Continuity Plan.	Yes () No ()
h) Indicate whether the event originated from a cybersecurity incident.	Yes () No ()
i) Indicate the impact of the events (according to the "Impact Scale"):	Very High <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low <input type="checkbox"/>
j) Is the Technological Infrastructure involved in the operational contingency managed by third parties?	Yes () No ()
k) If the answer to remark j) is yes, provide details of the provider and services provided.	

II. Classify the reported operational contingency based on the following causes that led to the operational contingencies:

Failures in the Technological Infrastructure that supports the services or Affection in the critical components of the Technological Infrastructure have had as a consequence the total or partial activation of the Business Continuity Plan.		
Failures or malfunctions		
Devices	Yes ()	No ()
Systems	Yes ()	No ()
Telecommunications	Yes ()	No ()
Services	Yes ()	No ()
Databases	Yes ()	No ()
Third-party equipment	Yes ()	No ()
Others (specify)		
Unintentional or accidental damage		
Errors in procedures or controls	Yes ()	No ()
Mention the procedures or controls		
Improper changes to data	Yes ()	No ()
Other(s):		

Cybersecurity incident		
Devices	Yes ()	No ()
Systems	Yes ()	No ()
Telecommunications	Yes ()	No ()
Services	Yes ()	No ()
Databases	Yes ()	No ()
Third-party equipment	Yes ()	No ()
Others (specify)		
Affection by scenarios other than those affecting the Technological Infrastructure		
Interruption or lack of supplies		
Manifestations	Yes ()	No ()
Strikes	Yes ()	No ()
Energy	Yes ()	No ()
Water	Yes ()	No ()
Others (specify)		
Natural or environmental disasters		
Earthquakes	Yes ()	No ()
Flooding	Yes ()	No ()
Hurricanes	Yes ()	No ()
Fires	Yes ()	No ()
Others (specify)		
Quantification caused by operational contingency		
Did the operational contingency cause a monetary loss to Clients or to the institution itself?	Yes ()	No ()
Monetary loss	\$	
Number of Clients affected		

IV. Report the description of the reported operational contingency.

a) Detailed description of the causes and diagnosis of the operational contingency (Indicate root cause and how it was determined).	
b) Actions implemented to solve the problems presented (corrective measures) (Indicate chronology and description of the actions taken).	
c) Indicate which controls failed.	
d) What preventive and corrective actions will be taken to mitigate the risk of an analogous situation occurring?	

e)	The work plan for corrective actions prepared for this purpose must contain at least the personnel responsible for their design, implementation, execution, and follow-up, deadlines for their execution, details of the activities carried out and to be carried out, as well as the technical resources, materials and human resources	
f)	Additional Information (Please indicate anything that you consider useful to complement this report).	

Name and signature of the representative of the Management Body.

In this Annex, part III must describe the reasons for classifying the incident based on the following "Impact Scale":

- "Critical" (i.e., disruption of essential business processes affecting other resources)
 - "High" (i.e., interruption of primary business processes)
 - "Medium" (i.e., it is possible to continue working using an alternative solution)
 - "Low" (i.e., interruption of secondary business processes)

ANNEX 6

Independent Third-Party Characteristics

A. Independence Requirements

It will be considered that there is no independence when the Independent Third Party or the legal entity through which it renders its services is located in any of the following cases:

- I. The Independent Third Party or the legal entity through which it provides its services exercises Control over the electronic payment funds institution, whether it is its subsidiary, its members, an entity with which it makes agreements with joint control, or a legal entity that belongs to the same Business Group or Consortium as the electronic payment funds institution.

The income received by the Independent Third Party or the legal entity through which it renders its services, coming from the electronic payment funds institution or, if applicable, from its holding company, subsidiaries, members, entities with which they make agreements with joint control or the legal entities that belong to the same Business Group or Consortium derived from the rendering of its services, represent, as a whole, 10% or more of the total income of such legal entity or Independent Third Party during the year immediately preceding the year in which it intends to render its services.

- II. The Independent Third Party or the legal entity through which it renders its services, has been a Client or important provider of the electronic payment funds institution or, as the case may be, of its holding company, subsidiaries, associates, entities with which they make agreements with joint control or legal entities that belong to the same Business Group or Consortium, during the year immediately before the year in which it intends to render the service.

A Client or provider is considered to be important when its sales or purchases to the electronic payment funds institution or, if applicable, to its holding company, subsidiaries, associates, entities with which they make agreements with joint control, or legal entities belonging to the same Business Group or Consortium, represent 10% or more of its total sales or, if applicable, total purchases.

- III. The Independent Third Party or any partner of the legal entity through which it renders its services is or has been during the year immediately before its hiring, a director, CEO, or employee occupying a position within the two levels immediately below the latter in the electronic payment funds institution, in its holding company, subsidiaries, associates, entities with which it makes agreements with joint control or legal entities belonging to the same Business Group or Consortium.
- IV. If the Independent Third Party or any partner of the legal entity through which the services are rendered, the spouse, concubine, or economic dependent of the aforementioned individuals, have investments in shares or debt securities issued by the

electronic payment funds institution or, as the case may be, by its holding company, subsidiaries, associates, entities with which they enter into agreements with joint control or legal entities belonging, have debt securities representing such shares or derivatives that have them as underlying, except in the case of time deposits, including certificates of deposit withdrawable on pre-established days, acceptances of banks or promissory notes with yields payable at maturity, provided that these are contracted under market conditions.

The provisions of this part must not apply to:

- a)** Holdings in shares representing the capital stock of equity investment funds and debt instruments.
 - b)** The holding of shares representing the capital stock of a corporation, registered in the National Securities Registry in charge of the National Banking and Securities Commission (CNBV), through trusts constituted for that sole purpose in which they do not intervene in the investment decisions, or securities referring to indexes or baskets of shares or in debt securities representing shares of the capital stock of two or more corporations issued under the protection of trusts.
- V.** The Independent Third Party or any partner of the legal entity through which the services are rendered, the spouse, concubine, or economic dependent of the aforementioned individuals, maintain with the electronic payment funds institution or, if applicable, with its holding company, subsidiaries, associates, entities with which they make agreements with joint control or legal entities that belong to the same Business Group or Consortium, debts for loans or credits of any nature, except in the case of credit card debts, financing for the purchase of durable consumer goods, mortgage loans for the acquisition of real estate and personal and payroll loans, as long as they are granted under market conditions.
- VI.** If the holding company, subsidiaries, associates, entities with which they make agreements with joint control, or legal entities that belong to the same Business Group or Consortium as the electronic payment funds institution have investments in the legal entity in which the Independent Third Party performing the audit provides its services or is a partner.
- VII.** If the Independent Third Party or the legal entity through which the services are rendered provides to the electronic payment funds institution, in addition to the compliance evaluation, any of the following services:
 - a)** Consultancy on the development of the processes, procedures, policies, and criteria, as well as the systems that the electronic payment funds institution must have in order to comply with the requirements referred to in these Provisions.
 - b)** Direct or indirect operation of financial information systems or administration of its local network.

- c)** Supervision, design, or implementation of computer systems (hardware and software) of the electronic payment funds institution, which carries out activities for the operations that the referred institution performs.
- d)** Supervision, design, or implementation of policies and procedures for information security, use of Instruction Channels, or operational continuity.
- e)** Provision of services related to information security, use of electronic media, or operational continuity.
- f)** Administration of the electronic payment funds institution, temporary or permanent, participating in the decisions.
- g)** Internal audit related to the evaluation of the level of compliance with the requirements related to information security, the use of Instruction Channels, and operational continuity.
- h)** Recruitment and selection of electronic payment funds institution personnel to fill positions of general director or the two levels immediately below the CEO.
- i)** Any other service that involves or could involve conflicts of interest concerning the compliance evaluation work performed.

VIII. The income that the Independent Third Party or the legal entity through which the service is rendered receives or will receive for carrying out the compliance evaluation of the electronic payment funds institution depends on the result of the assessment itself or on the success of any operation carried out by such electronic payment funds institution that is based on the compliance evaluation.

IX. The Independent Third Party, or the legal entity through which it provides the service, has overdue Accounts Receivable with the electronic payment funds institution for fees arising from any service that has already been provided to the electronic payment funds institution as of the date of issuance of the evaluation report.

B. Selection of the legal entity through which compliance assessment services will be provided.

The electronic payment funds institution must select a legal entity through which the Independent Third Party may provide compliance evaluation services to the standards contained in these Provisions, which must comply with the characteristics defined in this Annex.

If deemed convenient, the institution of electronic payment funds may select different legal entities to evaluate compliance with the requirements related to information security, use of Instruction Channels, and operational continuity.

If, as a result of the evaluation of the IT security and business continuity requirements, it is identified that one or more points are partially complied with or not complied with, any future assessment and as long as the observations are not entirely solved, must be carried out by the same legal entity that carried out the first evaluation.

Only when, for reasons of force majeure, the electronic payment funds institution cannot select the same legal entity, it may choose a different legal entity, for which it must fully justify its reasons in writing to Banco de México and the National Banking and Securities Commission (CNBV).

- C.** Service agreement made and entered into between the electronic payment funds institution and the legal entity through which compliance evaluation services will be rendered.

The electronic payment funds institution must establish a service agreement with the legal entity defining the terms under which the latter will perform the evaluation and the period that the activities will comprise. Such agreement must establish the following aspects:

- I.** The Independent Third Parties assigned to the project comply with the characteristics indicated in this Annex, as well as the established in these Provisions.
- II.** The delivery of the information between the electronic payment funds institution and the legal entity must be carried out under the terms specified in this Annex.
- III.** The information provided by the electronic payment funds institution and the compliance evaluation results may be required directly to the legal entity by Banco de México or the National Banking and Securities Commission (CNBV).
- IV.** The legal entity and the Independent Third Parties oblige to:
 - a)** Maintain confidentiality on the evidence collected and, on the results, obtained from evaluating the electronic payment funds institution on compliance with IT security and business continuity requirements.
 - b)** Maintain confidentiality regarding IT security and business continuity requirements.
 - c)** Safeguard the information produced as part of the evaluation in restricted access media to ensure its integrity and confidentiality.
- D.** Evaluation of compliance with the requirements related to information security, Instruction Channels, and business continuity.

Compliance evaluation comprises two types of reviews:

- I.** Extra-situ: Verification of documentary evidence provided by electronic payment funds institutions.
- II.** In-situ: Verification of compliance with the requirements through visits to the facilities of the electronic payment funds based on evidence provided by the institution.
- E.** Characteristics of the legal entity and Independent Third Party through which compliance evaluation services will be provided.

Independent Third Parties must comply with the following characteristics:

- I.** In the area of information security:

- a)** To have at least one of the following certifications: CISSP(Certified Information System Security Professional), CISA(Certified Information Systems Auditor), or CISM(Certified Information Security Manager) or their equivalents or those that replace them. Banco de México and the National Banking and Securities Commission (CNBV) may disclose the certifications that are equivalent to or replace those mentioned in this subsection on their websites.
- b)** Demonstrated at least two years of experience in information security consulting in the financial sector.
- c)** Have participated in activities or projects related to information security in the last twenty-four months.

II. In terms of business continuity:

- a)** Have at least two certifications: ISO 31000, ISO 22301, Basel II, and COSO II or their equivalents or those that replace them. Banco de México and the National Banking and Securities Commission (CNBV) may disclose the certifications that are equivalent to or replace those mentioned in this subsection on their websites.
- b)** Demonstrated experience in business continuity management auditing in the financial sector of at least two years.

The legal entity through which the Independent Third Party may provide services for the evaluation of compliance with the standards contained in these Provisions must meet the following characteristics:

- I.** Must not be disqualified from making and entering into any agreement with the Federal Public Administration for professional services related to information technology, operational risk, business continuity, and money laundering prevention.
- II.** In terms of information security, it must comply with the following:
 - a)** Experience in information security consulting in the financial sector of at least five years in the case of electronic payment funds institutions considered as relevant in accordance with these Provisions, Article 49.

For electronic payment funds institutions not considered within the aforementioned assumption, the independent third party must have at least two years of experience in information security matters in the financial sector or at least three years on such issues, but not specifically in the financial sector.

- b)** Profile oriented to information security auditing.

III. In terms of operational continuity, it must comply with the following:

- a)** Experience in risk management consulting in the financial sector of at least five (5) years in the case of electronic payment funds institutions considered relevant per the Provisions, Article 49.

For electronic payment funds institutions not considered within the aforementioned assumption, the independent third party must have at least two years of experience in information security matters in the financial sector or at least three years on such issues but not specifically in the financial sector.

b) Profile oriented to business continuity auditing.

IV. Independent Third Parties rendering services through the aforementioned legal entity must not be subcontracted.

ANNEX 7

Technical requirements to carry out Transactions through commission agents.

The commission agents or the Administrator of Commission Agents, to guarantee the correct execution of the Transactions and the security of the Information of the Clients, must have the following:


I. Definitions.

For this Annex, the following definitions must apply: Individual Identifier, the string of characters assigned to each operator.

II. Description of the technical characteristics of the systems, equipment, and applications that the commission agent or the Administrator of Commission Agents will use to carry out the Transactions, from the beginning to the allocation of the respective accounts of the electronic payment funds institution, considering all the participants involved.

The aforementioned description must contain at least the following:

- a)** Description of the communication links used by the electronic payment funds institution to connect with the commission agent, including at least the name of the commission agent, the bandwidth, and the type of Operation performed.
- b)** Telecommunications diagram showing the connection between each participant in the operation of the commission agent (service providers, data centers, electronic payment funds institution, among others), including redundancy schemes.
- c)** If applicable, scheme of the interrelation of applications or systems of the commission agent or the Administrator of Commission Agents, including the systems of the electronic payment funds institution.
- d)** Documentation showing the mechanisms to ensure the transmission of information in point-to-point encrypted form, including the version of the encryption protocols and security components of the Technological Infrastructure implemented in each node involved in the sending and receiving of data.
- e)** Detail of the type of information of the electronic payment funds institution,



of its Clients, or the users of means of disposition, specifying, if applicable, the type of Sensitive Information that will be stored by the commission agent or the Administrator of Commission Agents in their equipment or facilities, or to which they may have access. In the case of Sensitive Information, the commission agent or Administrator of Commission Agents must implement encryption mechanisms.

- f) Validation and testing procedure for the installation of the technological infrastructure of the commission agent.

Criteria related to the composition of the passwords or access keys of the operators and to the authentication factors for Clients or users through means of disposition, including personal identification numbers (PIN).

- III. Technological infrastructure requirements of the commission agent or Administrator of Commission Agents.

- a) Necessary mechanisms to carry out online transactions.

The technological infrastructure of the commission agent must have the necessary mechanisms to carry out online transactions in the case of receiving Process or withdrawal transactions, i.e., at the very moment the Transaction is carried out, updating the balances online of the Client in compliance with the operating rules of the electronic payment funds institutions themselves.

- b) Validation of the technological infrastructure of the commission agent.

Only the technological infrastructure of the commission agents authorized by the electronic payment funds institution will have access to the Technological Infrastructure provided by such institution (use of dedicated lines, identification of physical or logical addresses, VPNs, digital signatures, among others).

Likewise, the electronic payment funds institution must obtain evidence that the technological infrastructure used by the commission agents maintains control mechanisms that prevent the reading and extraction of the information of the Clients by unauthorized third parties.

- c) Policies and procedures for the administration of access and configuration of the technological infrastructure of the commission agents.

It is the responsibility of the electronic payment funds institution to have policies and procedures of the commission agent or Administrator of Commission Agents for:

1. The configuration of the technological infrastructure that connects to the computer systems of the electronic payment funds institution.
2. The administration of cryptographic keys used between the commission agents and the systems of the electronic payment funds institution.

- d) Creation of electronic records of Transactions.

All Transactions carried out through commission agents must generate electronic records that cannot be modified or erased and which must include, at least, the date, hour, and minute in which they were carried out, the type and amount of the instruction; if applicable, the account number of the Client, the means through which the instruction was carried out, as well as sufficient information to allow identifying the personnel who made the instruction. The custody of such records must be in charge of the electronic payment funds institution.

IV. Operator identification and Client authentication requirements.

- a) Necessary mechanisms for the full identification of commission agents.

In the development of Transactions through the commission agent, the electronic payment funds institutions must have mechanisms that allow them to identify the operators to have the necessary information for the resolution of clarifications or disputes. Such mechanisms must be indicated in the general operating plan referred to in these Provisions, Article 47, part I.

- b) Generation and delivery of passwords or access keys for operators.

The electronic payment funds institutions must establish mechanisms for the generation and delivery process of the authentication factors that ensure that only the commission agent or, as the case may be, its operators may know.

- c) Composition of operator passwords or access keys.

Criteria must be established for the length characteristics of operator passwords or access keys.

- d) Protection of operator passwords or access keys and Client Personal Identification Numbers (PINs).

The electronic payment funds institutions must provide the necessary measures to prevent the reading of the characters that make up the passwords or access keys of the operators, as well as the Personal Identification Numbers (PIN) entered by the Clients, respectively, in the technological

infrastructure of the commission agent, both in their capture and in their display on the screens.

Operator passwords or access keys and Client Personal Identification Numbers (PINs) must be validated and stored through encryption mechanisms. At no time can the commission agents access data related to the Personal Identification Numbers (PINs) of the Clients.

e) Two-factor authentication for Clients.

In order to carry out consultations and Transactions that represent a charge to the account of the Clients through the commission agents, the latter must authenticate themselves through the Technological Infrastructure of the commission agent with which such Transactions are carried out using an authentication factor referred to in these Provisions, Article 5, parts II and III.

For purposes of the foregoing, electronic payment funds institutions may opt for the combination of at least two of the following authentication factors and comply with these Provisions, Article 5.

f) For the reception and operation of transactions requested by Clients through the technological infrastructure of the commission agents, the operators must log in and authenticate themselves through such infrastructure.

The electronic payment funds institution must validate the authentication processes through the mechanisms and controls the institution deems convenient. The electronic payment funds institution must be responsible for ensuring that the commission agents have such operator authentication mechanisms in place to fulfill transactions.

V. Transaction of the technological infrastructure of the commission agent.

a) Generation of Transaction receipts.

The technological infrastructure of the commission agent must automatically generate the Transaction receipts issued by the electronic payment funds institutions for each Transaction, without any intervention by the personnel of the commission agent. Such Transaction receipts must be different from those used by commission agents to record the transactions inherent to their commercial activity.

When the transaction limits referred to in these Provisions, Article 48, are reached, as the case may be, the Transactions requested may not be carried out; therefore, the technological infrastructure of the commission agent must generate receipts indicating such a situation to the Client. For such purposes, a receipt must be provided with the following inscription:

“Transaction not carried out because it exceeded its permitted limit. Contact your electronic payment funds institution.”

The electronic payment funds institutions must attach the design of the receipt for each of the Transactions to be contracted.

Under no circumstances should the address of the Client be shown on the transaction receipt.

b) Transactions Monitoring.

The electronic payment funds institution must establish mechanisms that allow it to monitor the activities conducted by the operators through the technological infrastructure of the

commission agents to detect transactions that deviate from the usual Transaction parameters.

- c) Storage of the information of the Client in the technological infrastructure of the commission agent.

The commission agents may not store, keep, or copy in their technological infrastructure information of the Client of the electronic payment funds institution. In those cases, in which, for operational and technical reasons, it is required to store partially or totally such information in its technological infrastructure, it must have encryption mechanisms.

The electronic payment funds institutions must be responsible for verifying compliance with this subsection.

Annex 8

Specifications of the information system developed by a third party for the information encryption shared with the National Banking and Securities Commission and Banco de México.

For the purposes of this Annex, capitalized terms used herein, in singular or plural, must have the same meanings as those established for such terms in the Code of Commerce and the Extended Security Infrastructure (ISE) Rules, as well as the following:

Qualified Digital Certificate:

a Digital Certificate issued, in accordance with the Extended Security Infrastructure (ISE) Rules, by the Tax Administration Service, in its capacity as Certification Agency, also referred to in the provisions thereof as “electronic signature,” which is stored in a digital file with extension “.cer” when it is obtained before such authority following the provisions established for such purpose, as well as that other Digital Certificate that, per the Extended Security Infrastructure (ISE) Rules, is issued by a third party authorized, if applicable, by Banco de México, subject to the determination of the latter that such Digital Certificate complies with the exact security requirements and accreditation of the identity of the interested party as observed by the Tax Administration Service for

Encryption:

its issuance.
The process of applying Qualified Electronic Signature Verification Data to a Data Message to generate a new one that is incomprehensible to any person, except for the Holder of the Qualified Digital Certificate of which the Qualified Electronic Signature Verification Data is part, who, in turn, serves as the Recipient of such Data Message.

Creation of an Electronic Signature:

The process of applying Qualified Electronic Signature Creation Data to a Data Message and generating the Electronic Signature that is added to the Data Message.

Qualified Electronic Signature Creation Data:

The Electronic Signature Creation Data foreseen in the Extended Security Infrastructure (ISE) Rules that the Holder generates as part of the issuance process of its respective Digital Certificate, which is stored in a digital file with a ".key" extension.

Qualified Electronic Signature Verification Data:

The Electronic Signature Verification Data referred to in the Extended Security Infrastructure (ISE) Rules are part of the information in the Digital Certificate.

Decryption:

The process of applying Qualified Electronic Signature Creation Data to a Data Message that has been Encrypted so that the Holder of the respective Digital Certificate can view the content of the original Data Message.

Electronic Signature:

The set of data that is added to a Data Message, which is logically associated with it and is attributable to the Holder once the Qualified Information System has been used and that complies with the requirements of Advanced or Reliable Electronic Signature referred to in the Code of Commerce, Article 89, as subsequently amended or replaced.

Extended Security Infrastructure (ISE):

The one referred to in the Extended Security Infrastructure (ISE) Rules.

Extended Security Infrastructure (ISE) Rules:

The Rules for Operating as a Registration Agency and/or Certification Agency in the Extended Security Infrastructure, issued by Banco de México through Official Communication-Telefax 6/2005, as subsequently modified or replaced.

Qualified Information System:

The information system that allows, on the one hand, the Creation of Electronic Signatures as an Electronic Signature Creation Device in terms of the Extended Security Infrastructure (ISE) Rules and, on the other hand, the Verification of Electronic Signatures as an Electronic Signature Verification Device in terms of such Rules, as well as to carry out the Encryption and Decryption of Data Messages.

Holder:

The person referred to in the Extended Security Infrastructure (ISE) Rules who intervenes in his capacity as Signatory in terms of the Code of Commerce, Article 89.

**Verification of an
Electronic Signature:**

The process of applying the Electronic Signature Verification Data to the Electronic Signature of a Data Message and verifying both the reliability of such Electronic Signature by proving that it was created for that same Data Message using the Electronic Signature Creation Data corresponding to the Electronic Signature Verification Data, and the integrity of the Data Message by not being altered after its Electronic Signature has been generated.

The computer program developed by a third party to perform the Encryption of information shared with the National Banking and Securities Commission (CNBV) and Banco de México must comply with the following specifications:

- I. Its principal function is the application of cryptographic algorithms that comply with the Electronic Signature specifications set forth in the Extended Security Infrastructure (ISE) Rules.

Maintain communication with a Registration Agency of the Extended Security Infrastructure to be able to request and verify the validity of Qualified Digital Certificates of the Signatories involved in the processes of Creation and Verification of Electronic Signatures and encrypt and decrypt Data Messages. For this purpose, the computer program must comply with the Communication Protocol with the Extended Security Infrastructure that the General Directorate of Payment Systems and Market Infrastructures maintains at the disposal of interested parties on the page that Banco de México has on its website identified with the domain www.banxico.org.mx.

- II. Implement the Taxpayer Identification Number 3852 “Cryptographic Message Syntax (CMS)” standard for creating an Electronic Signature and encrypting Data Messages. Within the referred standard, the specification of the file resulting from the Creation of an Electronic Signature generated through the so-called Signed-data Content Type on the information made up of the data type files whose specification in its ASN.1 notation is described below. Likewise, within the referred standard, the specification of the file resulting from the encryption of a Data Message is generated using the so-called Enveloped-data Content Type on the information made up of the data type files whose specification in its ASN.1 notation is described below.
- The information used within the Taxpayer Identification Number 3852 standard is that which is arranged according to the following description in ASN.1 notation:

```
Files ::= SEQUENCE of Archive
File ::= SEQUENCE {
    name OCTET STRING,
    content OCTET STRING }
```

where **name** is the name of the file containing the information of interest. On the other hand, **content** is the information included in that file interpreted as a sequence of bytes.