1. Purpose

The purpose of this document is to establish the regulatory framework for information security for INDEA supplier organizations that access INDEA information, information systems or resources, in order to protect their confidentiality, integrity, availability, authenticity and traceability.

To this end, supplier organizations are responsible for informing their employees and subcontractors who provide services to INDEA.

2. Scope

All activities carried out for INDEA by supplier organizations that access its information, information systems or resources.

Section "3. General Guidelines" applies to any supplier organization, regardless of the type of service provided.

Section "4. Specific Guidelines" applies exclusively to supplier organizations whose services correspond to the type of service indicated in each case, as stated at the beginning of that section.

3. General Guidelines

3.1. Service Provision

Supplier organizations may only perform for INDEA those activities covered under the corresponding service provision contract.

The supplier organization shall periodically provide INDEA with the list of people, profiles, functions and responsibilities associated with the service provided, and shall promptly report any change (addition, removal, replacement or change of functions or responsibilities) occurring in that list.

In accordance with the clauses associated with the service provision contract, all external persons working for INDEA must comply with the security rules set out in this document. In the event of a breach of any of these obligations, INDEA reserves the right to veto the person who committed the infringement, as well as to adopt any sanctioning measures deemed appropriate in relation to the supplier organization.

The supplier organization shall ensure that all its personnel have the appropriate training to perform the service provided.

Any exchange of information between INDEA and the supplier organization shall be understood to have been carried out within the framework established by the corresponding service provision contract, and such information may not be used outside that framework or for other purposes.

IT centralizes the overall efforts to protect INDEA assets.

In general terms, assets include:

- Protected information, i.e. information that makes it possible to identify natural and/or legal persons, and information relating to the configuration of information systems and communication networks.

- The assets associated with processing protected information (software, hardware, communication networks, information media, auxiliary equipment and facilities).

3.2. Information Confidentiality

External persons who have access to INDEA information must consider that such information is protected by default. Only information accessed through public information dissemination channels provided for that purpose by INDEA may be considered unprotected information.

The disclosure, modification, destruction or misuse of information shall be avoided, regardless of the medium in which it is held.

The strictest confidentiality shall be maintained indefinitely, and protected information shall not be disclosed externally unless duly authorized.

The number of paper reports containing protected information shall be minimized and they shall be kept in a secure place out of reach of third parties.

If, for reasons directly related to the job, an employee of the supplier organization comes into possession of protected information contained in any type of medium, they must understand that such possession is strictly temporary, subject to a duty of secrecy, and does not grant them any right of possession, ownership or copy over that information. The employee must also return the aforementioned medium or media immediately after completion of the tasks that gave rise to their temporary use and, in any case, upon termination of their company's relationship with INDEA.

All these obligations shall remain in force after the end of the activities performed by external persons for INDEA.

Failure to comply with these obligations may constitute an offence of disclosure of secrets.

To guarantee the security of personal data, personnel of the supplier organization must observe the following rules of conduct, in addition to the considerations already mentioned:

- Files may only be created when necessary to perform their work. These temporary files must never be stored on local disk drives of users' PCs and must be destroyed when they are no longer useful for the purpose for which they were created.

- Personal data shall not be hosted on local disk drives of users' PCs.

- The removal of media and documents (including sending e-mails) from the premises where such information is located may only be authorized by INDEA and shall be carried out according to the defined procedure.

- Media and documents must make it possible to identify the type of information they contain, be inventoried and be stored in a place with access restricted to authorized persons.

- The transmission of specially protected personal data (e.g. health data) through telecommunications networks (e.g. e-mail) shall be carried out by encrypting such data or by using any other mechanism that ensures the information is not intelligible to, or manipulated by, third parties.

3.3. Intellectual Property

Compliance with legal restrictions on the use of material protected by intellectual property regulations shall be guaranteed.

Users may only use material authorized by INDEA for the performance of their duties.

The use of computer programs without the corresponding license on INDEA information systems is strictly prohibited.

Likewise, the use, reproduction, assignment, transformation or public communication of any type of work or invention protected by intellectual property without due written authorization is prohibited.

INDEA shall only authorize the use of material produced by INDEA itself, or material authorized or supplied to it by its owner, in accordance with the agreed terms and conditions and applicable regulations.

3.4. Information Exchange

No person shall conceal or manipulate their identity under any circumstances.

The distribution of information, whether in electronic or physical format, shall be carried out using the resources determined in the service provision contract for that purpose and solely for the purpose of facilitating the functions associated with that contract. Depending on the identified risk, INDEA reserves the right to implement control, logging and audit measures over these dissemination resources.

In relation to the exchange of information within the framework of the service provision contract, the following activities shall be considered unauthorized:

- Transmission or receipt of material protected by copyright in breach of intellectual property law.

- Transmission or receipt of any kind of pornographic material, sexually explicit material, racially discriminatory statements and any other kind of statement or message classifiable as offensive or illegal.

- Transfer of protected information to unauthorized third parties.

- Transmission or receipt of non-business applications.

- Participation in Internet activities, such as newsgroups, games or others that are not directly related to the provision of the service.

All activities that may damage INDEA's image and reputation are prohibited on the Internet and elsewhere.

3.5. Appropriate Use of Resources

The supplier organization undertakes to periodically inform INDEA of the assets with which it provides the service.

The supplier organization undertakes to use the resources provided for the service in accordance with the conditions for which they were designed and implemented.

The resources that INDEA makes available to external persons, regardless of their type (IT resources, data, software, networks, communication systems, etc.), are available exclusively to fulfill the obligations and purpose of the operation for which they were provided. INDEA reserves the right to implement control and audit mechanisms to verify the appropriate use of these resources.

All equipment of the supplier organization that connects to INDEA's production network shall be of approved brands and models. The supplier organization shall make such equipment available to INDEA so that INDEA can coordinate installation of the approved software and configure it appropriately.

Any file introduced into the INDEA network or into any equipment connected to it through automated media, the Internet, e-mail or any other means must comply with the requirements established in these rules and, in particular, those relating to intellectual property, personal data protection and malware control.

All assets must be returned to INDEA without undue delay after termination of the contract. All personal computers on which INDEA has installed software shall be taken to INDEA so that the hard disk can be formatted at the end of the service.

The following are expressly prohibited:

- Use of the resources provided by INDEA for activities not related to the purpose of the service.

- Connection to INDEA's production network of equipment and/or applications that are not specified as part of the software or the standards for the supplier's own IT resources.

- Introducing obscene, threatening, immoral or offensive content into INDEA's information systems or corporate network.

- Voluntarily introducing into INDEA's corporate network any type of malware (viruses, worms, Trojans, spyware, ransomware, etc.), logical device, physical device or any other type of command sequence that causes or may cause any type of alteration or damage to IT resources. All persons with access to the INDEA network shall be required to use updated antimalware programs.

- Obtaining, without explicit authorization, rights or access other than those assigned by INDEA.

- Accessing restricted areas of INDEA information systems without explicit authorization.

- Distorting or falsifying the logs of INDEA information systems.

- Decrypting, without explicit authorization, encryption keys, systems or algorithms and any other security element involved in INDEA telematic processes.

- Possessing, developing or running programs that could interfere with the work of other users or damage or alter INDEA IT resources.

- Destroying, altering, disabling or otherwise damaging data, programs or electronic documents containing protected information (these acts may constitute an offence).

- Hosting protected information on local disk drives of users' PCs.

3.6. User Responsibilities

Supplier organizations must ensure that all persons working for INDEA observe the following basic principles in their activities:

- Each person with access to INDEA information is responsible for the activity carried out under their user ID and everything arising from it. Therefore, each person must keep the authentication systems associated with their user ID under control, ensuring that the associated password is known only by that user and must not be disclosed to anyone under any circumstances.

- Users must not use another user's identifier, even if authorized by the owner.

- Users know and apply the requirements and procedures existing around the information handled.

Any person with access to protected information must follow the following directives regarding password management:

- Select quality passwords, i.e. passwords that are difficult for other users to guess.

- Request a password change whenever there is any possible indication that other users may know it.

- Change passwords at least once every 90 days and avoid reusing old passwords.

- Change default and temporary passwords at first login.

- Avoid including passwords in automated login processes (e.g. those stored in browsers).

- Report any security incident related to passwords, such as loss, theft or any indication of loss of confidentiality.

Any person with access to protected information must ensure that equipment is protected when left unattended.

Any person with access to protected information must observe at least the following clean desk rules, in order to protect paper documents, computer media and portable storage devices and reduce the risks of unauthorized access, loss and damage to information, both during normal working hours and outside them:

- Store paper documents and computer media under lock and key when not in use, especially outside working hours.

- Lock user sessions or turn off the PC when leaving it unattended.

- Protect both information receiving and sending points (postal mail, scanner and fax machines) and duplication equipment (photocopier, fax and scanner). The reproduction or sending of information using this type of device shall be the responsibility of the user.

- Remove any protected information without undue delay once printed.

- Destroy protected information once it is no longer needed.

- Persons with access to INDEA systems and/or information must never, without written authorization, perform tests to detect and/or exploit a suspected weakness, security event or incident.

- No person with access to INDEA systems and/or information shall attempt, by any means and without express written authorization, to breach the security system and authorizations. Network traffic capture by users is prohibited unless authorized audit tasks are being carried out in writing.

All persons who access protected information must follow the following rules of conduct:

- Protect protected information from any unauthorized disclosure, modification, destruction or misuse, whether accidental or not.

- Protect all information systems and telecommunications networks against unauthorized access or use, operational interruptions, destruction, misuse or theft.

- Have the necessary authorization to obtain access to information systems and/or information.

3.7. User Equipment

Supplier organizations must ensure that all user IT equipment used to access protected information complies with the following rules:

- After user inactivity, the equipment must lock automatically within a maximum of 15 minutes.

- No user equipment shall have tools that could breach security systems and authorizations.

- User equipment shall be maintained in accordance with the manufacturer's specifications.

- All user equipment shall be adequately protected against malware:

o Antimalware software must be installed and used on all personal computers to reduce the operational risk associated with viruses or other malicious software.

o They shall be kept up to date with the latest available security updates.

o Antimalware software must always be enabled and updated.

Special attention shall be paid to the security of all mobile user equipment that contains protected information or allows access to it in any way:

- Verifying that it does not include more information than is strictly necessary.

- Ensuring that access controls are applied to that information.

- Minimizing access to that information in the presence of persons outside the service provided.

- Transporting the equipment in covers, briefcases or similar equipment that incorporates appropriate protection against environmental agents.

3.8. Hardware Equipment Management

Supplier organizations must ensure that all equipment provided by INDEA for the provision of services, regardless of type, is properly managed. To this end, they must comply with the following rules:

- The supplier organization must maintain an up-to-date list of equipment provided by INDEA and the users of those assets, or associated responsible persons if the assets are not for single-person use. This list may be requested by INDEA.

- Whenever a supplier organization wishes to reassign any INDEA equipment that has contained protected information, it must temporarily return it so that the necessary secure erasure procedures can be carried out before reassignment.

- If a supplier organization wishes to remove any item from the list of INDEA equipment received, it must always return it so that INDEA can handle that removal appropriately.

- If a supplier organization ceases to provide the service, it must return to INDEA the full list of equipment received, as established in the corresponding service provision contracts. Only in the case of paper documents and computer media may the supplier organization proceed with secure disposal, in which case it must notify INDEA of such disposal.

4. Specific Guidelines

4.1. Scope of Application

All supplier organizations must comply, in addition to the general rules, with the specific rules set out in this section that apply to them in each case, depending on the characteristics of the service provided to INDEA.

The types of service covered are indicated below.

- Place of service execution: Depending on the main place where the services are performed, two cases are distinguished:

o INDEA: The supplier organization provides the service mainly from INDEA's own premises.

o Remote: The supplier organization provides the service mainly from its own premises, although occasional activities may be carried out at INDEA's premises.

- Ownership of the ICT infrastructures used: Depending on who owns the main ICT infrastructures (communications, user equipment, software) used to provide the service, two cases are distinguished:

o INDEA.

o Supplier organization.

- Level of access to INDEA systems: Depending on the level of access to INDEA information systems, three cases are distinguished:

o With privileged access: The service provided requires privileged access to INDEA information systems, with the ability to administer those systems and/or the production data they process.

o With user-level access: The service provided requires the use of INDEA information systems, so that the persons providing the service have user accounts that allow them to access some of those systems with standard privileges.

o No access: The service provided does not require the use of INDEA information systems, so the persons providing the service do not have user accounts on those systems.

Depending on each of the three categories into which each service falls, the supplier organization must comply, in addition to the general security rules, with the specific rules set out in the sections indicated in the following table:

	LOCATION		*INFRASTRUCTURE*		*ACCESS*		
	INDEA	*Remote*	*INDEA*	*Supplier organization*	*Privileged*	*Standard*	*No access*
personnel selection	NO	NO	NO	NO	YES	NO	NO
security audit	NO	NO	NO	NO	YES	NO	NO
incident communication	YES	YES	YES	NO	YES	YES	NO
physical security	NO	YES	NO	NO	NO	NO	NO
asset management	NO	NO	NO	YES	NO	NO	NO
security architecture	NO	NO	NO	YES	YES	YES	NO
system security	NO	NO	NO	YES	NO	NO	NO
network security	NO	NO	NO	YES	NO	NO	NO

	LOCATION		*INFRASTRUCTURE*		*ACCESS*		
	INDEA	*Remote*	*INDEA*	*Supplier organization*	*Privileged*	*Standard*	*No access*
traceability of system use	NO	NO	NO	YES	YES	NO	NO
identity and access control and management	NO	NO	NO	YES	NO	NO	NO
change management	NO	NO	NO	YES	YES	YES	NO
technical change management	NO	NO	NO	NO	YES	NO	NO
development security	NO	NO	NO	NO	YES	YES	NO
contingency management	NO	NO	NO	YES	NO	NO	NO

4.2. Personnel Selection

The supplier organization must verify the professional background of the persons assigned to the service, guaranteeing to INDEA that in the past they have not been sanctioned for professional malpractice or been involved in incidents relating to the confidentiality of the information processed that resulted in any kind of sanction.

The supplier organization must guarantee INDEA the possibility of immediately removing from the service any person assigned to it in relation to whom INDEA wishes to exercise the right of veto, in accordance with the conditions established in section "3.1. Service Provision".

4.3. Security Audit

The supplier organization must allow INDEA to carry out the requested security audits, cooperating with the audit team and providing all evidence and records requested.

The scope and depth of each audit shall be expressly established by INDEA in each case. Audits shall be carried out according to the planning agreed in each case with the supplier organization providing the service.

INDEA reserves the right to carry out additional extraordinary audits whenever specific justified reasons exist.

4.4. Incident Communication

When any information security vulnerability, event and/or incident is detected, it must be reported immediately through the INDEA e-mail mailbox.

Any user may submit through that mailbox any events, suggestions, vulnerabilities, etc. that may relate to information security and the guidelines set out in these rules of which they are aware.

Any incident detected that affects or may affect the security of personal data must be reported through that mailbox (e.g. loss of lists and/or computer media, suspicions of misuse of authorized access by other persons, recovery of data from backup copies, etc.).

That mailbox centralizes the collection, analysis and management of reported incidents.

If the mailbox cannot be accessed, the communication channels established within the service itself must be used, so that the INDEA contact person communicates the security incident.

4.5. Physical Security

The premises must be closed and must have an access control system.

There shall be some form of visitor control, at least in public access areas and/or loading and unloading areas.

The premises must have at least adequate fire detection and extinguishing systems, and must be built in such a way as to provide sufficient resistance to flooding.

If any type of backup copy is maintained, the systems that host and/or process such information must be located in a specially protected area that includes at least the following security measures:

- The specially protected area must have an access control system independent from that of the premises.
- Access by external persons to specially protected areas shall be limited. Such access shall be assigned only when necessary and authorized, and always under the supervision of authorized persons.
- A record of all access by external persons shall be maintained.
- External persons may not remain or perform work in specially protected areas without supervision.
- The consumption of food or beverages in these specially protected areas shall be prohibited.
- Systems located in these areas must have some type of protection against power failures.

4.6. Asset Management

The supplier organization must have an up-to-date asset register in which the assets used to provide the service can be identified.

All assets used to provide the service must have a responsible person, who must ensure that those assets incorporate the minimum security measures established by the supplier organization, which must at least be those specified in these regulations.

The supplier organization must notify INDEA of removals of assets used to provide the service. If such asset contains other INDEA property (hardware, software or any other type of asset), it must be delivered to INDEA before removal so that INDEA can withdraw the assets it owns.

Whenever an asset has contained protected information, the supplier organization must carry out asset removals ensuring secure deletion of that information, applying secure erasure functions or physically destroying the asset so that the information it contained cannot be recovered.

4.7. Security Architecture

Whenever the supplier organization performs application development and/or testing work for INDEA or with protected information, the environments in which these activities are carried out must be isolated from each other and also isolated from production environments where protected information is hosted or processed.

All access to information systems that host or process protected information must be protected at least by a firewall that limits connection capability to them.

Information systems that host or process specially sensitive information must be isolated from the rest.

4.8. System Security

Information systems that host or process protected information must record the most significant events relating to their operation. These activity records shall be covered by the supplier organization's backup policy.

The clocks of the supplier organization's systems that process or host protected information shall be synchronized with each other and with the official time.

The supplier organization shall ensure that the capacity of information systems that store or process protected information is properly managed, avoiding potential shutdowns or malfunctions of those systems due to resource saturation.

Information systems that host or process protected information shall be adequately protected against malicious software by applying the following precautions:

- Systems shall be kept up to date with the latest available security updates in development, testing and production environments.

- Antimalware software must be installed and used on all servers and personal computers to reduce the risk associated with malicious software.

- Antimalware software must always be enabled and updated.

The supplier organization shall establish a backup policy that guarantees the safeguarding of any data or information relevant to the service provided, on a weekly basis.

Whenever e-mail is used in relation to the service provided, the supplier organization must respect the following premises:

- The transmission of protected information by e-mail shall not be permitted unless the electronic communication is encrypted and the sending is authorized in writing.

- The transmission by e-mail of information containing specially protected personal data (e.g. health data) shall not be permitted unless the electronic communication is encrypted and the sending is authorized in writing.

- Whenever INDEA e-mail is used to provide the service, at least the following principles must be respected:

- E-mail shall be considered another work tool provided exclusively for the contracted service. This consideration shall authorize INDEA to implement control systems intended to ensure the protection and proper use of this resource. This authority shall nevertheless be exercised while safeguarding people's dignity and their right to privacy.

- INDEA's e-mail system must not be used to send fraudulent, obscene, threatening or similar messages.

- Users must not create, send or forward advertising or pyramid messages (messages that spread to multiple users).

Access to information systems that host or process protected information must always be authenticated, at least through the use of a personal identifier and an associated password.

Information systems that host or process protected information must have access control systems that limit access to such information exclusively to service personnel.

Access sessions to information systems that host or process protected information must lock automatically after a certain period of user inactivity.

Whenever software provided by INDEA is used, the following rules must be observed:

- All persons accessing INDEA information systems must use only the software versions provided and follow their rules of use.

- All persons are prohibited from installing illegal copies of any software.

- The use of software not validated by INDEA is prohibited.

- Uninstalling any of the programs installed by INDEA is also prohibited.

4.9. Network Security

Networks through which protected information circulates must be appropriately managed and controlled, ensuring that there are no uncontrolled accesses or connections whose risks are not properly managed by the supplier organization.

The services available on networks through which protected information circulates must be limited as far as possible.

Networks that allow access to INDEA's ICT infrastructure must be properly protected, and the following premises must be met:

- Remote user access to the INDEA network shall be subject to compliance with prior identification and authentication procedures and access validation.

- These connections shall be made for a limited time and using virtual private networks or dedicated lines.

- No type of communication equipment (cards, modems, etc.) that enables uncontrolled alternative connections shall be permitted in these connections.

Access to networks through which protected information circulates must be limited.

All equipment connected to networks through which protected information circulates must be properly identified, so that network traffic can be identifiable.

Remote working, considered as access to the corporate network from outside, is regulated by applying the following rules:

- The use of equipment not controlled by INDEA for remote working activities is not permitted.

- Remote working authorization criteria shall be established based on the needs of the job.

- The necessary measures for secure connection to the corporate network shall be established.

- Security monitoring and audit systems shall be established for the connections made.

- The revocation of access rights and return of equipment after the end of the period of need shall be controlled.

Whenever Internet access provided by INDEA is used, the following additional rules must be observed:

- The Internet is a work tool. All Internet activities must be related to work tasks and activities. Users must not search for or visit sites that do not support INDEA's business objective or the performance of their daily work.

- Internet access from the corporate network shall be restricted by control devices incorporated into it. The use of other means of connection must be previously validated and shall be subject to the preceding considerations on Internet use.

- Users must not use INDEA's name, symbol, logo or similar symbols in any Internet element (e-mail, web pages, etc.) unless justified by strictly work-related activities.

- Data transfer to or from the Internet shall only be permitted when related to business activities. File transfer unrelated to these activities (e.g. downloading programs, multimedia files, etc.) shall be prohibited.

4.10. Traceability of System Use

Privileged accesses shall be logged, and those logs shall be retained in accordance with the Organization's backup policy.

The activity of the systems used to carry out such privileged access shall be logged, and those logs shall be retained in accordance with the Organization's backup policy.

Errors and failures recorded in system activity shall be analyzed, and the necessary measures shall be adopted to remedy them.

4.11. Identity and Access Control and Management

All users with access to an information system shall have a single access authorization composed of a user ID and password.

Users shall be responsible for all activity related to the use of their authorized access.

Users must not use another user's authorized access, even if authorized by the owner.

Users must not disclose their identifier and/or password to another person under any circumstances, nor keep it written down in view or within reach of third parties.

The minimum password length shall be 6 characters and it must not contain the user's first name, surname or user ID. It must be changed every 45 days and at least the previous 8 passwords must not be repeated.

They must also be complex and difficult to guess, and therefore must be made up of a combination of at least 3 of these 4 options in the first 8 characters:

- Uppercase letters
- Lowercase letters
- Numbers
- Special characters

It is advisable to use the following guidelines for password selection:

- Do not use known words or words that may be associated with oneself, for example a name.
- The password must not refer to any recognizable concept, object or idea. Therefore, passwords should avoid using significant dates, days of the week, months of the year, names of people, telephone numbers, etc.
- The password should be practically impossible to guess. At the same time, it should be easy for the user to remember. A good example is to use the acronym of a phrase or expression.

The supplier organization must ensure that it periodically verifies that only duly authorized persons have access to protected information.

In cases where INDEA information systems are also accessed, the following rules must also be considered:

- No user shall receive an access identifier for INDEA systems until they have accepted the current security regulations in writing.

- Users shall have authorized access only to the data and resources they need to perform their duties.

- If the system does not request it automatically, the user must change the provisional password assigned the first time they make a valid access to the system.

- If the system does not request it automatically, the user must change their password at least once every 90 days.

- Temporary authorized accesses shall be configured for a short period of time. Once that period has expired, they shall be disabled in the systems.

- In relation to personal data, only persons authorized to do so may grant, change or cancel authorized access to data and resources, in accordance with the criteria established by the file controller.

- If a user suspects that their authorized access (user ID and password) is being used by another person, they must change their password and report the incident to the INDEA e-mail mailbox.

4.12. Change Management

All changes to the ICT infrastructure must be controlled and authorized, ensuring that uncontrolled components do not form part of it.

It must be verified that all new components introduced into the supplier organization's ICT infrastructure used to provide the service operate properly and fulfill the purposes for which they were incorporated.

4.13. Technical Change Management

All changes carried out must follow a formally established and documented procedure that ensures the appropriate steps are followed to make the change.

The change management procedure must ensure that changes to the ICT infrastructure are minimized and limited to those strictly necessary.

All changes must be tested before deployment in the production environment, to verify that no adverse collateral or unforeseen effects occur on the operation and security of the ICT infrastructure.

Supplier organizations must scan and mitigate technical vulnerabilities in the infrastructures used to provide the service, informing INDEA of all those associated with critical components.

4.14. Development Security

The entire outsourced software development process shall be controlled and supervised by INDEA.

Identification, authentication, access control, audit and integrity mechanisms shall be incorporated throughout the software design, development, implementation and operation life cycle.

The software specifications must expressly contain the security requirements to be covered in each case.

The software developed must incorporate input data validations that verify that the data is correct and appropriate and that prevent the introduction of executable code.

Internal processes developed by applications must incorporate all validations necessary to ensure that information corruption does not occur.

Whenever necessary, authentication and integrity control functions must be incorporated into communications between the different application components.

The output information offered by applications must be limited, ensuring that only relevant and necessary information is provided.

Access to application source code must be limited to service personnel.

In the testing environment, real data shall only be used when it has been appropriately dissociated or whenever it can be guaranteed that the security measures applied are equivalent to those existing in the production environment.

During application testing, it shall be verified that there are no uncontrolled information breaches and that only the intended information is provided through the established channels.

Only software that has been expressly approved shall be transferred to the production environment.

In relation to Web services, management of the OWASP Top 10 shall be considered.

4.15. Contingency Management

The service must have a plan that allows it to be provided even in the event of contingencies.

The previous plan must be developed according to the events capable of causing service interruptions and their probability of occurrence.

The supplier organization must be able to demonstrate the viability of the existing contingency plan.

5. Monitoring and Control

In order to ensure the proper use of the aforementioned resources, through the formal and technical mechanisms deemed appropriate, INDEA shall verify this, either periodically or when advisable for specific security or service reasons.