Secure information management standard for suppliers

1. Purpose:

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

To do so, supplier organisations are responsible for informing their employees and subcontractors who provide services to the Organisation.

2. Outreach

All activities carried out for the Organisation by supplier organisations that access its information, information systems or resources.

General guidelines" is applicable to any provider organisation, regardless of the type of service provided.

Specific guidelines" is applicable only to those provider organisations whose services provided correspond to the type of service indicated in each case, as indicated at the beginning of the aforementioned section.

3. General guidelines

3.1. Service provision

Supplier organisations may only perform for the Organisation those activities covered under the relevant service contract.

In accordance with the provisions of the clauses associated with the service contract, all external persons carrying out work for the Organisation shall comply with the security standards set out in this document. In the event of non-compliance with any of these obligations, the Organisation reserves the right to veto the person who has committed the infraction, as well as the adoption of the sanctioning measures considered appropriate in relation to the provider organisation.

The provider organisation shall ensure that all its persons have the appropriate training for the performance of the service provided.

Any type of exchange of information that takes place between the Organisation and the supplier organisation shall be understood to have been carried out within the framework established by the corresponding service provision contract, so that this information may not be used outside this framework or for other purposes.

The operations and product departments centralise the overall efforts to protect the organisation's assets.

Generically, assets include:

- Protected information, i.e. information that allows the identification of natural and/or legal persons, and information relating to the configuration of information systems and communications networks.
- Those associated with the processing of protected information (software, hardware, communications networks, information media, auxiliary equipment and installations).

3.2. Confidentiality of the information

External persons who have access to the Organisation's information shall, by default, consider such information to be protected information. Only information to which access has been obtained through the means of public dissemination of information provided for this purpose by the Organisation may be considered as unprotected information.

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

Maximum confidentiality shall be maintained indefinitely and protected information shall not be released to the outside world unless duly authorised.

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

In the event that, for reasons directly related to the job, the employee of the supplier organisation comes into possession of protected information contained in any type of support, he/she shall understand that such possession is strictly temporary, with an obligation of secrecy and without this conferring any right of possession, ownership or copying of such information. Likewise, the employee must return the aforementioned media immediately upon completion of the tasks that have given rise to the temporary use thereof and, in any case, upon termination of the relationship with his or her company's Organisation.

All these obligations shall continue to apply after the termination of the activities that the external persons carry out for the Organisation.

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

In order to ensure the security of personal data, the following rules of conduct shall be observed by the persons of the supplying organisation, in addition to the considerations already mentioned:

- They may only create files when necessary for the performance of their work. These temporary files shall never be stored on the local disk drives of users' PC workstations and shall be destroyed when they are no longer useful for the purpose for which they were created.
- No personal data shall be stored on the local disk drives of the user's PC workstations.
- The removal of media and documents (including the sending of e-mails), outside the premises where such information is located, may only be authorised by the Organisation and shall be carried out in accordance with the defined procedure.
- The media and documents must allow the type of information they contain to be identified, be inventoried and stored in a place to which access is restricted to authorised persons.
- The transmission of specially protected personal data (e.g. health) via telecommunications networks (e.g. e-mail) shall be carried out by encrypting such data or using any other mechanism that guarantees that the information cannot be intelligible or manipulated by third parties.

3.3. Intellectual property

Compliance with legal restrictions on the use of material protected by copyright law will be ensured.

Users may only use material authorised by the Organisation for the performance of their duties.

The use of software without the corresponding licence on the Organisation's information systems is strictly prohibited.

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

The Organisation will only authorise the use of material produced by itself, or material authorised or supplied to it by its owner, in accordance with the terms and conditions agreed and the provisions of the regulations in force.

3.4. Exchange of information

No person shall conceal or manipulate his or her 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 this purpose and for the exclusive purpose of facilitating the functions associated with this contract. the Organisation reserves the right, depending on the risk identified, to implement control, recording and auditing measures on these dissemination resources.

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

- Transmission or receipt of copyright-protected material in violation of the Law on Intellectual Protection.
- Transmission or receipt of any kind of pornographic material, sexually explicit material, racially discriminatory statements and any other kind of statement or message that can be classified as offensive or illegal.
- Transfer of protected information to unauthorised third parties.
- Transmission or receipt of non-business related applications.
- Participation in Internet activities such as newsgroups, games or other activities not directly related to the provision of the service.

All activities that may damage the image and reputation of the Organisation are prohibited on the Internet and elsewhere.

3.5. Appropriate use of resources

The provider organisation undertakes to periodically inform the Organisation of the assets with which it provides the service.

The provider organisation undertakes to use the resources made available for the provision of the service in accordance with the conditions for which they were designed and implemented.

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

All Supplier Organisation equipment connected to the Organisation's production network shall be of approved makes and models. The supplier organisation shall make such equipment available to the Organisation to co-ordinate the installation of the approved software and configure it appropriately.

Any file introduced into the Organisation's network or into any equipment connected to it by means of automated media, Internet, electronic mail or any other means, must comply with the requirements established in these regulations and, in particular, those referring to intellectual property, protection of personal data, and malware control.

All assets shall be returned to the Organisation without undue delay after termination of the contract. All personal computers that have had software installed on them by the Organisation shall be taken to the Organisation to have the hard drive formatted upon termination of the service.

It is expressly prohibited:

- The use of the resources provided by the Organisation for activities not related to the purpose of the service.
- The connection to the Organisation's production network of equipment and/or applications that are not specified as part of the software or standards of the Organisation's own IT resources.
- Introducing obscene, threatening, immoral or offensive content into the Organisation's information systems or corporate network.
- Voluntarily introducing into the Organisation's corporate network any type of malware (viruses, worms, Trojans, spyware, ransomware, etc.), logical device, physical device or any other type of sequence of commands that cause or are likely to cause any type of alteration or damage to computer resources. All persons with access to the Organisation's network are obliged to use up-to-date anti-malware software.
- Obtain without explicit authorisation rights or access other than those assigned to them by the Organisation.
- Gaining access without explicit authorisation to restricted areas of the Organisation's information systems.
- Distort or falsify the Organization's information systems log records.
- Decrypt without explicit authorisation the encryption keys, systems or algorithms and any other security element involved in the Organisation's telematic processes.
- Possess, develop or execute programs that could interfere with the work of other users, or damage or alter the Organisation's computer resources.
- Destroy, alter, disable or otherwise damage data, programs or electronic documents containing protected information (such acts may constitute a criminal offence).
- Host protected information on the local disk drives of user PC workstations.

3.6. Responsibilities of the User

Service-providing organisations shall ensure that all persons performing work for the organisation respect the following basic principles within their activity:

- Each person with access to the Organisation's information is responsible for the activity carried out by his or her user identifier and all that derives from it. Therefore, it is essential that each person maintains control of the authentication systems associated with their user identifier, guaranteeing that the associated password is only known to the user and must not be revealed to others under any circumstances.
- Users must not use any identifier belonging to another user, even if they have the owner's authorisation.
- Users are aware of and apply existing requirements and procedures relating to the information they handle.
- Anyone with access to protected information should follow the following guidelines in relation to password management:
- Select quality passwords, i.e. passwords that are difficult to guess by other users.
- Ask for the password to be changed whenever there is a possible indication of knowledge by other users.
- Change passwords at least once every 90 days and avoid reusing old passwords.
- Change default and temporary passwords on first login.
- Avoid including passwords in automated login processes (e.g. those stored in browsers).
- Report any security incidents related to your passwords such as loss, theft or indications of loss of confidentiality.

- Anyone with access to protected information should ensure that computers are protected when they are to be left unattended.
- Anyone with access to protected information should observe at least the following clean desk rules, in order to protect paper documents, computer media and portable storage devices and to reduce the risks of unauthorised access, loss and damage to information, both during and outside normal working hours:
- Store paper documents and computer media under lock and key when not in use, especially outside working hours.
- Lock user sessions or switch off the PC when it is left unattended.
- Protect both the points where information is received and sent (postal mail, scanner and fax machines) and the duplication equipment (photocopier, fax and scanner). The reproduction or sending of information with this type of device is the responsibility of the user.
- Remove, without undue delay, any protected information once printed.
- Destroy protected information once it is no longer needed.
- Persons with access to the Organisation's systems and/or information shall never, without written authorisation, conduct tests to detect and/or exploit a suspected security weakness, event or incident.
- No person with access to the Organisation's systems and/or information shall, without express written authorisation, attempt by any means to breach the security system and authorisations. The capture of network traffic by users is prohibited, except in the case of audit work authorised in writing.
- All persons accessing protected information must follow the following rules of conduct:
- Protect protected information from unauthorised disclosure, modification, destruction or misuse, whether accidental or not.
- Protect all information systems and telecommunications networks against unauthorised access or use, disruption of operations, destruction, misuse or theft.
- Have the necessary authorisation to gain access to information systems and/or information.

3.7. User equipment

Service provider organisations shall ensure that all user computer equipment used to access protected information complies with the following standards:

Upon user inactivity, the equipment shall be automatically locked within a maximum of 15 minutes.

No user equipment shall be equipped with tools that could breach security systems and authorisations.

- User equipment shall be maintained in accordance with the manufacturer's specifications.
- All personal user equipment shall be adequately protected against malware:
    - Anti-malware software shall be installed and used on all personal computers to reduce the operational risk associated with viruses or other malicious software.
    - They shall be kept up to date with the latest available security updates.
    - Anti-malware software shall always be enabled and kept up to date.
- Special care shall be taken to ensure the security of all user mobile equipment that contains or otherwise allows access to protected information:
- Verifying that they do not contain more information than is strictly necessary.
- Ensuring that access controls are applied to such information.
- Minimising access to such information in the presence of persons not involved in the service provided.
- Transporting equipment in cases, briefcases or similar equipment that incorporates appropriate protection against environmental agents.

3.8. Hardware management

Service provider organisations shall ensure that all equipment provided by the organisation for the provision of services, regardless of its type, is properly managed. To this end, they shall comply with the following standards:

- The provider organisation shall maintain an up-to-date list of equipment provided by the Organisation and persons using such assets, or associated responsible persons in case the assets are not for sole use. Such a list may be required by the Organisation.
- Whenever a Provider Organisation wishes to reassign any of the Organisation's equipment that has contained Protected Information, it shall temporarily return such equipment so that the necessary secure deletion procedures can be carried out prior to reassignment.
- In the event that a Provider Organisation wishes to remove any equipment received from the Organisation's equipment list, it must always return the equipment, so that the Organisation can deal with such removal appropriately.
- In the event that a provider organisation ceases to provide the service, it must return to the Organisation the entire 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 Organisation securely dispose of them, in which case it shall notify the Organisation of such disposal.

4. Specific directives

4.1. Scope of application

All supplier organisations shall 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 the Organisation.

The types of service contemplated are those indicated below.

- Place of execution of the service: Depending on the main place where the services are carried out, two cases can be distinguished:
  - the Organisation: The provider organisation provides the service mainly from the organisation's own headquarters.
  - Remote: The provider organisation provides the service mainly from its own premises, although occasional activities may be carried out at the organisation's headquarters.
- 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 can be distinguished:
  - the Organisation.
  - Provider organisation.
- Level of access to the organisation's systems: Depending on the level of access to the Organisation's information systems, three cases can be distinguished:
  - With privileged access: The service provided requires privileged access to the Organisation's information systems, with the capacity to administer these systems and/or the production data they process.
  - o With user-level access: The service provided requires the use of the Organisation's information systems, so that the persons providing the service have user accounts that allow them to access some of these systems with normal privileges.
  - No access: The service provided does not require the use of the Organisation's information systems, so the persons providing the service do not have user accounts on these systems..

Depending on each of the three categories into which each service falls, the provider organisation must comply, in addition to the general safety standards, with the specific standards set out in the sections indicated in the following table:

	LOCATION		***INFRASTRUCTURE***		***ACCESS***		
	Organization	*Remote*	*Organization*	*Supplier*	*Privileged*	*Normal*	*No access*
selection of persons	NO	NO	NO	NO	YES	NO	NO
security auditing	NO	NO	NO	NO	YES	NO	NO
incident reporting	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
systems security	NO	NO	NO	YES	NO	NO	NO
network security	NO	NO	NO	YES	NO	NO	NO
systems usage traceability	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. Scope of application

The supplier organisation shall verify the professional background of the persons assigned to the service, guaranteeing to the Organisation that in the past they have not been sanctioned for professional malpractice nor have they been involved in incidents related to the confidentiality of the information processed that have led to any type of sanction.

The provider organisation must guarantee to the Organisation the possibility of immediate removal from the persons assigned to the service of any person in relation to whom the Organisation wishes to exercise the right of veto, in accordance with the conditions set out in section "3.1.

4.3. Security audit

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

audits, cooperating with the audit team and providing all required evidence and records.

as may be required.

The scope and depth of each audit shall be expressly established by the Organisation on a case-by-case basis.

each case. The audits shall be carried out according to the schedule agreed in each case with the organisation providing the service.

with the organisation providing the service.

The Organisation reserves the right to carry out additional extraordinary audits, provided that.

4.4. Incident reporting

When any information security vulnerability, event and/or incident is detected, it must be notified immediately through the e-mail box: seguridadinformacion@ludusglobal.com

Any user may report through the aforementioned mailbox any events, suggestions, vulnerabilities, etc. that may be related to information security and the guidelines contemplated in these rules of which he/she becomes aware.

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

The mailbox centralises the collection, analysis and management of reported incidents.

If access to the mailbox is not available, the communication channels established within the service itself should be used, so that the Organisation's interlocutor is the one to report the security incident.

4.5. Physical security

The site shall be gated and shall have some form of access control system.

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

The site shall have at least adequate fire detection and suppression systems and shall be constructed to provide sufficient resistance to flooding.

If any backup is maintained, the systems housing and/or processing such information should be located in a specially protected area, which includes at least the following security measures:

- The specially protected area shall have a separate access control system from that of the headquarters.
- Access to persons outside the specially secured area shall be limited. Such access shall be granted only when necessary and authorised, and always under the supervision of authorised persons.
- A record shall be kept of all access by outsiders.
- Outsiders may not remain or carry out work in the specially protected areas without supervision.
- The consumption of food or drink in these specially protected areas shall be prohibited.
- Systems located in these areas shall have some form of power failure protection.

4.6. Asset management

The provider organisation shall have an up-to-date asset register in which the assets used for the provision of the service can be identified.

All assets used for the provision of the service shall have a responsible person, who shall ensure that such assets incorporate the minimum security measures established by the provider organisation, which shall at least be those specified in these regulations.

The provider organisation shall notify the Organisation of the disposal of assets used for the provision of the service. If the asset contains other property of the Organisation (hardware, software or other types of assets), it shall be handed over to the Organisation prior to decommissioning so that the Organisation can remove the assets from its property.

Whenever an asset has contained protected information, the Provider Organisation shall carry out asset retirement by ensuring the secure disposal of such information, by applying secure deletion functions or by physically destroying the asset, so that the information contained therein cannot be recovered.

4.7. Security architecture

Whenever the service provider organization carries out development and/or testing of applications for the Organization or with protected information, the environments with which such activities are carried out must be isolated from each other and also isolated from the production environments in which protected information is housed or processed.

All access to information systems housing or processing protected information shall be protected at least by a firewall, which limits the ability to connect to them.

Information systems that house or process particularly sensitive information must be isolated from the rest.

4.8. System security

Information systems that house or process protected information shall record the most significant events surrounding their operation. These activity logs shall be covered by the provider organization's backup policy.

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

The service provider organization shall ensure that the capacity of the information systems that store or process protected information is adequately managed, avoiding potential downtime or malfunctions of such systems due to resource saturation.

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

- Systems shall be kept up to date with the latest available security updates, in development, test and production environments.
- Anti-malware software shall be installed and used on all servers and personal computers to reduce the risk associated with malicious software.
- Anti-malware software shall always be enabled and up to date.

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

Whenever e-mail is used in connection with the service provided, the provider organization must respect the following premises:

- Protected information may not be transmitted via e-mail unless the electronic communication is encrypted and the transmission is authorized in writing.
- The transmission via e-mail of information containing specially protected personal data (e.g. Health) shall not be permitted, unless the electronic communication is encrypted and the sending is authorized in writing.
- Whenever the Organization's e-mail is used to provide the service, at least the following principles shall be observed:
- E-mail shall be considered as one more work tool provided for the exclusive purpose of the contracted service. This consideration shall entitle the Organization to implement control systems designed to ensure the protection and proper use of this resource. This power, however, shall be exercised while safeguarding the dignity of individuals and their right to privacy.
- The Organization's e-mail system shall not be used to send fraudulent, obscene, threatening or other similar communications.
- Users must not create, send or forward advertising or pyramid messages (messages that are sent to multiple users).

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

Information systems that house or process protected information shall have access control systems that limit access to such information to service persons only.

Access sessions to information systems that house or process protected information shall be automatically blocked after a certain period of inactivity by users.

Whenever software provided by the Organization is used, the following rules must be followed:

- All persons accessing the Organization's information systems must use only the software versions provided and following its rules of use.
- All persons are prohibited from installing illegal copies of any software.
- The use of software not validated by the Organization is prohibited.
- It is also forbidden to uninstall any of the software installed by the Organization.

4.9. Network security

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

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

The networks that allow access to the organization's ICT infrastructure must be appropriately protected, and the following requirements must be met:

- Access by remote users to the organization's network shall be subject to compliance with prior identification and authentication procedures, and validation of access.
- These connections will be made for a limited time and through the use of virtual private networks or dedicated lines.
- No communications equipment of any kind (cards, modems, etc.) will be allowed in these connections that allow alternative, uncontrolled connections.
- Access to the networks through which the protected information circulates must be limited.
- All equipment connected to the networks through which the protected information circulates must be appropriately identified, so that network traffic can be identifiable.

- Teleworking, considered as access to the corporate network from the outside, is regulated by the application of the following regulations:
- The use of equipment not controlled by the Organization for teleworking activities is not allowed.
- Criteria will be established for the authorization of teleworking based on the needs of the job.
- The necessary measures will be established for secure connection to the corporate network.
- Security monitoring and auditing systems will be established for the established connections.
- The revocation of access rights and return of equipment after the end of the period of need for this will be controlled.
- Whenever Internet access provided by the Organization is used, the following rules must also be observed:
- The Internet is a working tool. All Internet activities must be related to work tasks and activities. Users must not search for or visit sites that do not support the Organization's business objective or the performance of their daily work.
- Access to the Internet from the corporate network will be restricted by means of control devices incorporated in the same. The use of other means of connection must be previously validated and shall be subject to the above considerations on the use of the Internet.
- Users must not use the Organization's name, symbol, logo or similar symbols in any Internet element (e-mail, Web pages, etc.) not justified by strictly work-related activities.
- The transfer of data to or from the Internet shall only be permitted when related to business activities. The transfer of files not related to these activities (e.g. downloading of programs, multimedia files, etc.) shall be prohibited..

4.10. Network security

Privileged access shall be logged and records shall be kept in accordance with the Organization's backup regulations.

The activity of the systems used to carry out such privileged access shall be recorded, and such records shall be kept in accordance with the Organization's backup regulations.

Errors and failures recorded in the activity of the systems shall be analyzed and the necessary measures shall be taken 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 consisting of a user ID and password.

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

Users shall not use any authorized access of another user, even if authorized by the owner.

Under no circumstances shall users disclose their user ID and/or password to any other person, nor shall they keep it in writing in plain view or within the reach of third parties.

The minimum length of the password must be 6 characters and must not contain the name, surname or identifier of the user. It must be changed every 45 days and must not repeat at least the previous 8 passwords.

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

- Uppercase
- Lowercase
- Numbers
- Special characters

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

- Do not use familiar words, or words that can be associated with oneself, for example, one's name.
- The password should not refer to any recognizable concept, object or idea. Therefore, you should avoid using significant dates, days of the week, months of the year, names of people, telephone numbers, ... in your passwords.
- The password should be something practically impossible to guess. But at the same time it should be easily remembered by the user. A good example is to use the acronym of some phrase or expression.
- The provider organization must ensure that it is periodically verified that only duly authorized persons have access to the protected information.
- In those cases in which the organization's information systems are also accessed, the following regulations must also be considered:
- No user shall be given an access ID to the Organization's systems until he/she agrees in writing to the security regulations in force.
- Users shall have authorized access only to those data and resources they require for the performance of their duties.
- If the system does not automatically request it, the user must change the temporary password assigned to him/her the first time he/she accesses the system.
- If the system does not automatically request it, the user must change the assigned temporary password the first time he/she makes a valid access to the system.
- In the event that the system does not automatically request it, the user must change his/her password at least once every 90 days.
- Temporary authorized accesses shall be set up for a short period of time. Once this period has expired, they will be deactivated from the systems.
- In relation to personal data, only authorized persons may grant, alter or revoke authorized access to data and resources, in accordance with the criteria established by the person responsible for the file.
- If a user suspects that his/her authorized access (user ID and password) is being used by another person, he/she must change his/her password and notify the incident to the e-mail address seguridadinformacion@ludusglobal.com.

4.12. Management of changes

All changes to the ICT infrastructure shall be controlled and authorized, ensuring that no uncontrolled components are part of it.

All new components introduced into the provider organization's ICT infrastructure used to provide the service must be verified to ensure that they function properly and fulfill the purposes for which they were incorporated.

4.13. Technical change management

All changes that are made shall be carried out following a formally established and documented procedure that ensures that the appropriate steps are followed to make the change.

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

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

The supplier organizations shall scan and mitigate the technical vulnerabilities presented by the infrastructures used for the provision of the service, informing the Organization of all those associated with critical components.

4.14. Safety in development

The entire outsourced software development process will be controlled and supervised by the Organization.

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

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

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

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

Whenever necessary, authentication and integrity control functions should be incorporated into communications between the different components of the applications.

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

Access to the source code of the applications shall be limited to service personnel.

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

During the testing of the applications, it shall be verified that there are no uncontrolled information gaps, 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, the management of the Owasp Top 10 (https://owasp.org/www-project-top-ten/) will be considered.

4.15. Contingency management

The service shall have a plan that allows its provision even in case of contingencies.

The above plan shall be developed based on the events capable of causing service interruptions and their probability of occurrence.

The provider organization shall be able to demonstrate the viability of the existing contingency plan.

5. Follow-up and control

In order to ensure the correct use of the aforementioned resources, through the formal and technical mechanisms deemed appropriate, the Organization will check, either periodically or when it is convenient for specific security or service reasons.

MIKEL CEARSOLO CABREJAS CEO LUDUS TECH S.L.

Ludus

ludusglobal.com

Ludus Tech, S.L.
C.I.F. B-95661856

+34 946 12 22 41