

### 1. Purpose

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

To this end, supplier organisations are responsible for informing their employees and subcontractors who provide services to Grupo Azpiaran.

### 2. Scope

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

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

Section "4. Specific guidelines" applies exclusively to those supplier organisations whose services correspond to the type of service indicated in each case, as indicated at the beginning of the aforementioned section.

### 3. General guidelines

#### 3.1. Provision of the service

Supplier organisations may only carry out activities for the Azpiaran Group that are covered by the corresponding service provision contract.

The service provider organisation shall periodically provide Grupo Azpiaran with a list of the persons, profiles, functions and responsibilities associated with the service provided, and shall promptly report any changes (new hires, departures, replacements or changes in functions or responsibilities) that occur in this list.

In accordance with the provisions of the clauses associated with the service provision contract, all external persons carrying out work for the Azpiaran Group must comply with the security regulations set out in this document. In the event of non-compliance with any of these obligations, Grupo Azpiaran reserves the right to veto the person who has committed the infringement, as well as to adopt the disciplinary measures deemed appropriate in relation to the supplier organisation.

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

Any exchange of information between Grupo Azpiaran and the supplier organisation 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 this framework or for other purposes.

IT centralises the global efforts to protect Grupo Azpiaran's assets

In general terms, 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.
- Associates for the processing of protected information (software, hardware, communications networks, information media, auxiliary equipment and facilities).

### **3.2. Confidentiality of information**

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

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

The utmost confidentiality shall be maintained indefinitely and no protected information shall be disclosed to outside parties unless duly authorised.

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

In the event that, for reasons directly related to their job, an employee of the supplier organisation comes into possession of protected information contained in any type of medium, they must understand that such possession is strictly temporary, with an obligation of secrecy and without conferring any right of possession, ownership or copying of such information. Likewise, the employee must return the aforementioned media immediately after completing the tasks that gave rise to their temporary use and, in any case, upon termination of their company's relationship with Grupo Azpiaran.

All these obligations shall remain in force after the end of the activities carried out by external persons for Grupo Azpiaran.

Failure to comply with these obligations may constitute a crime of disclosure of secrets.

To ensure the security of personal data, persons within the supplier organisation must observe the following rules of conduct, 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 local disk drives of users' PCs and must 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 users' PCs.
- The removal of media and documents (including sending emails) from the premises where such information is located may only be authorised by Grupo Azpiaran and shall be carried out in accordance with the defined procedure.
- Media and documents must allow the type of information they contain to be identified, be inventoried and stored in a location with restricted access to authorised persons.

- The transmission of specially protected personal data (e.g. health) via telecommunications networks (e.g. email) shall be carried out by encrypting such data or using any other mechanism that ensures that the information cannot be understood 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 authorised by Grupo Azpiaran for the performance of their duties.

The use of computer programs without the corresponding licence on Grupo Azpiaran'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 rights without the proper written authorisation is prohibited.

Grupo Azpiaran will only authorise the use of material produced by itself, or material authorised or supplied to it by its owner, in accordance with the agreed terms and conditions and the provisions of current legislation.

### **3.4. Exchange of information**

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 specified in the service provision contract for this purpose and for the sole purpose of facilitating the functions associated with said contract. Grupo Azpiaran reserves the right, depending on the risk identified, to implement control, registration and audit 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 unauthorised:

- Transmission or reception of material protected by copyright in violation of the Intellectual Property Law.
- Transmission or reception of any kind of pornographic material, of an explicitly sexual nature, 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 reception of applications unrelated to the business.
- 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 the image and reputation of Grupo Azpiaran are prohibited on the Internet and elsewhere.

### **3.5. Appropriate use of resources**

The provider organisation undertakes to periodically inform Grupo Azpiaran 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 Grupo Azpiaran makes available to external parties, regardless of their type (computers, data, software, networks, communication systems, etc.), are available exclusively for the fulfilment of the obligations and purpose of the operation for which they were provided. Grupo Azpiaran reserves the right to implement control and audit mechanisms to verify the appropriate use of these resources.

All equipment belonging to the supplier organisation that connects to the Grupo Azpiaran production network must be of approved brands and models. The supplier organisation shall make such equipment available to Grupo Azpiaran so that it can coordinate the installation of the approved software and configure it appropriately.

Any file introduced into the Grupo Azpiaran network or any equipment connected to it via automated media, the Internet, email or any other means must comply with the requirements set out in these rules and, in particular, those relating to intellectual property, personal data protection and malware control.

All assets must be returned to Grupo Azpiaran without undue delay after the termination of the contract. All personal computers on which Grupo Azpiaran has installed software shall be taken to Grupo Azpiaran for the hard drive to be formatted at the end of the service.

The following are expressly prohibited:

- The use of resources provided by Grupo Azpiaran for activities unrelated to the purpose of the service.
- Connecting equipment and/or applications that are not specified as part of the software or standards of the company's own IT resources to the Grupo Azpiaran production network.
- Introducing obscene, threatening, immoral or offensive content into Grupo Azpiaran's information systems or corporate network.
- Voluntarily introducing any type of malware (viruses, worms, Trojans, spyware, ransomware, etc.), logical device, physical device or any other type of command sequence that causes or is likely to cause any type of alteration or damage to IT resources into the Grupo Azpiaran corporate network. All persons with access to the Azpiaran Group network shall be required to use up-to-date anti-malware programmes.
- Obtaining, without explicit authorisation, rights or access other than those assigned to them by Grupo Azpiaran.
- Accessing restricted areas of Grupo Azpiaran's information systems without explicit authorisation.
- Distorting or falsifying the log records of Grupo Azpiaran's information systems.
- Deciphering, without explicit authorisation, the passwords, systems or encryption algorithms and any other security element involved in Grupo Azpiaran's telematic processes

- Possess, develop or execute programmes that could interfere with the work of other users, or damage or alter the computer resources of Grupo Azpiaran
- Destroy, alter, disable or in any other way damage data, programmes or electronic documents containing protected information (these acts may constitute a criminal offence).
- Storing protected information on the local hard drives of user PCs.

### **3.6. User responsibilities**

Service provider organisations must ensure that all persons working for Grupo Azpiaran respect the following basic principles in their activities:

- Each person with access to Grupo Azpiaran information is responsible for the activity carried out by their user ID and everything that derives from it. Therefore, it is essential that each person keeps the authentication systems associated with their user ID under control, ensuring that the associated password is known only to the user themselves and must not be disclosed to other persons under any circumstances.
- Users must not use any other user's identifier, even if they have the owner's authorisation.
- Users are aware of and apply the existing requirements and procedures regarding the information handled.

Anyone with access to protected information must follow the following guidelines regarding password management:

- Select high-quality passwords, i.e. those that are difficult for other users to guess.
- Request a password change whenever there is a possible indication that other users may have gained knowledge of it.
- Change passwords at least once every 90 days and avoid reusing old passwords.
- Change default and temporary passwords upon 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 signs of a breach of confidentiality.

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

Anyone with access to protected information must comply with at least the following clean desk rules in order to protect paper documents, computer media and portable storage devices and 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 shut down the PC when leaving it unattended.
- Protect both information reception and transmission points (postal mail, scanners and fax machines) and duplication equipment (photocopiers, fax machines and scanners). The reproduction or transmission of information using these types of devices is the responsibility of the user.

- Remove any protected information once printed without undue delay.
- Destroy protected information once it is no longer needed.
- Persons with access to Grupo Azpiaran systems and/or information shall never, without written authorisation, carry out tests to detect and/or exploit a suspected security weakness, event or incident.
- No person with access to Grupo Azpiaran systems and/or information shall attempt, without express written authorisation, to breach the security system and authorisations by any means. The capture of network traffic by users is prohibited, unless authorised written audit tasks are being carried out.

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 otherwise.
- Protect all information systems and telecommunications networks against unauthorised access or use, interruption of operations, destruction, misuse or theft.
- Obtain the necessary authorisation to access information systems and/or information.

### **3.7. User equipment**

Service providers must ensure that all user equipment used to access protected information complies with the following standards:

- When the user is inactive, the equipment must automatically lock within a maximum of 15 minutes.
- No user equipment shall have tools that could breach security systems and authorisations.
- User equipment shall be maintained in accordance with the manufacturer's specifications.
- All user equipment shall be adequately protected against malware:
  - o Anti-malware 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 security updates available.
  - o Anti-malware software must always be enabled and updated.

Special care shall be taken to ensure the security of all user mobile devices that contain protected information or allow access to it in any way:

- 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 outside the service provided.
- Transporting equipment in cases, briefcases or similar equipment that provides appropriate protection against environmental agents.

### **3.8. Hardware equipment management**

Service providers must ensure that all equipment provided by Grupo Azpiaran for the provision of services, regardless of type, is managed appropriately. To this end, they must comply with the following rules:

- The supplier organisation must maintain an up-to-date list of equipment provided by Grupo Azpiaran and the users of such assets, or the persons responsible for them if the assets are not for single-user use. This list may be requested by Grupo Azpiaran.
- Whenever a supplier organisation wishes to reassign any Grupo Azpiaran equipment that has contained protected information, it must return it temporarily so that the necessary secure deletion procedures can be carried out prior to its reassignment.
- If a supplier organisation wishes to remove any of the equipment received from Grupo Azpiaran from the list of equipment, it must always return it so that Grupo Azpiaran can process the removal appropriately.
- If a supplier organisation ceases to provide the service, it must return all the equipment received to Grupo Azpiaran, as established in the corresponding service provision contracts. Only in the case of paper documents and computer media may the supplier organisation proceed with their secure disposal, in which case it must notify Grupo Azpiaran of such disposal.

#### **4. Specific guidelines**

##### **4.1. Scope**

In addition to the general rules, all supplier organisations must comply 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 Grupo Azpiaran.

The types of service covered are those indicated below.

- Place of service provision: Depending on the main place where the services are provided, there are two cases:
  - o Grupo Azpiaran: The supplier organisation provides the service mainly from Grupo Azpiaran's own headquarters.
  - o Remote: The provider organisation mainly provides the service from its own premises, although specific activities may be carried out at the Grupo Azpiaran headquarters.
- Ownership of the ICT infrastructure used: Depending on who owns the main ICT infrastructure (communications, user equipment, software) used to provide the service, there are two possible scenarios:
  - o Grupo Azpiaran
  - o Providing organisation.
- Level of access to Grupo Azpiaran systems: Depending on the level of access to Grupo Azpiaran's information systems, there are three different cases:
  - o With privileged access: The service provided requires privileged access to Grupo Azpiaran's information systems, with the ability to administer those systems and/or the production data they process.

- o User-level access: The service provided requires the use of Grupo Azpiaran's information systems, so that the persons providing the service have user accounts that allow them to access any of these systems with normal privileges.
  - o No access: The service provided does not require the use of Grupo Azpiaran's information systems, so that the persons providing the service do not have user accounts on those systems.
- Depending on which of the three categories each service falls into, the provider organisation 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		
	Azpiaran Group	Remote	Azpiaran Group	Supplier organisation	Privileged	Standard	No access
Selection of individuals	NO	NO	NO	NO	YES	NO	NO
security audit	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
architecture security	NO	NO	NO	YES	YES	YES	NO
security systems	NO	NO	NO	YES	NO	NO	NO
network security	NO	NO	NO	YES	NO	NO	NO
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	NO	NO	NO	NO	YES	NO	NO

	LOCATION		INFRASTRUCTURE		ACCESS		
	Azpiaran Group	Remote	Azpiaran Group	Supplier organisation	Privileged	Standard	No access
management							
security in development	NO	NO	NO	NO	YES	YES	NO
contingency management	NO	NO	NO	YES	NO	NO	NO

### 4.2. Selection of personnel

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

The supplier organisation must guarantee Grupo Azpiaran the possibility of immediately removing any persons assigned to the service in relation to whom Grupo Azpiaran wishes to exercise its right of veto, in accordance with the conditions set out in section "3.1. Provision of the service".

### 4.3. Security audit

The provider organisation must allow Grupo Azpiaran to carry out the requested security audits, collaborating with the audit team and providing all the evidence and records required.

The scope and depth of each audit shall be expressly established by Grupo Azpiaran in each case. Audits shall be carried out in accordance with the plan agreed in each case with the service provider organisation.

Grupo Azpiaran reserves the right to carry out additional extraordinary audits, provided that there are specific reasons that justify them.

### 4.4. Incident reporting

When any vulnerability, event and/or information security incident is detected, it must be reported immediately via the Grupo Azpiaran email address.

Any user may use this mailbox to report any events, suggestions, vulnerabilities, etc. that may be related to information security and the guidelines set out in these rules of which they are aware.

Any incident that is detected and that affects or may affect the security of personal data (e.g. loss of lists and/or computer media, suspected misuse of authorised access by other persons, recovery of data from backups, etc.) must be reported via the aforementioned mailbox.

The aforementioned 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 must be used, so that the Grupo Azpiaran representative can report the security incident.

### **4.5. Physical security**

The headquarters must be locked and must 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 premises must have, at a minimum, adequate fire detection and extinguishing systems, and must be constructed in such a way as to offer sufficient resistance to flooding.

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

- The specially protected area must have an access control system that is independent of that of the headquarters.
- Access to specially protected areas shall be restricted to external persons. 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 external persons.
- External persons may not remain or carry out work in specially protected areas without supervision.
- The consumption of food or drink in these specially protected areas will be prohibited.
- Systems located in these areas must have some form of protection against power failures.

### **4.6. Asset management**

The provider organisation 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 designated person responsible for ensuring that they incorporate the minimum security measures established by the provider organisation, which must be at least those specified in these regulations.

The provider organisation must notify Grupo Azpiaran of any decommissioning of assets used to provide the service. If such assets contain other property belonging to Grupo Azpiaran (hardware, software or other types of assets), they must be handed over to Grupo Azpiaran prior to decommissioning so that Grupo Azpiaran can proceed to remove the assets belonging to it.

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

### **4.7. Security architecture**

Whenever the service provider organisation carries out application development and/or testing work for Grupo Azpiaran or with protected information, the environments in which such activities are carried out must be isolated from each other and also isolated from the production environments in which protected information is stored or processed.

All access to information systems that host or process protected information must be protected by at least a firewall, which limits the ability to connect to them.

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

### **4.8. System security**

Information systems that store or process protected information must record the most significant events related to their operation. These activity logs shall be covered by the backup regulations of the provider organisation.

The clocks of the provider organisation's systems that process or store protected information shall be synchronised with each other and with the official time.

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

Information systems that host 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 security updates available in development, testing 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 must always be enabled and updated.

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

Whenever email is used in connection with the service provided, the provider organisation must comply with the following requirements:

- The transmission of protected information via email shall not be permitted unless the electronic communication is encrypted and the transmission is authorised in writing.
- The transmission of information containing specially protected personal data (e.g. health) via email shall not be permitted unless the electronic communication is encrypted and the transmission is authorised in writing.
- Whenever Grupo Azpiaran's email is used to provide the service, at least the following principles must be respected:
  - Email shall be considered as another work tool provided for the sole purpose of the contracted service. This consideration shall entitle Grupo Azpiaran to implement control systems

designed to ensure the protection and proper use of this resource. This power shall, however, be exercised in a manner that safeguards the dignity of individuals and their right to privacy.

- The Grupo Azpiaran email system must not be used to send fraudulent, obscene, threatening or other similar messages.
- Users shall not create, send or forward advertising or pyramid messages (messages that are sent to multiple users).

Access to information systems that store or process protected information must always be authenticated, at least by means of a personal identifier and an associated password.

Information systems that store 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 store or process protected information must be automatically blocked after a certain period of user inactivity.

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

- All persons accessing Grupo Azpiaran's 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 Grupo Azpiaran is prohibited.
- It is also prohibited to uninstall any of the programmes installed by Grupo Azpiaran.

### **4.9. Network security**

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

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

Networks that allow access to the Azpiaran Group's ICT infrastructure must be adequately protected, and the following premises must be met:

- Access by individuals and remote users to the Azpiaran Group network shall be subject to compliance with identification and authentication procedures and access validation.
- These connections shall be for a limited time and shall be made using virtual private networks or dedicated lines.
- No type of communications equipment (cards, modems, etc.) that enables alternative uncontrolled connections will be permitted on these connections.

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

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

Teleworking, considered as access to the corporate network from outside, is regulated by the application of the following regulations:

- The use of equipment not controlled by Grupo Azpiaran for teleworking activities is not permitted.

- Criteria for authorising teleworking will be established based on the needs of the job.
- The necessary measures for secure connection to the corporate network will be established.
- Security monitoring and auditing systems will be established for the connections established.
- The revocation of access rights and the return of equipment after the period of need has ended will be monitored.

Whenever use is made of the Internet access provided by Grupo Azpiaran, the following regulations must also 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 Grupo Azpiaran's business objectives or the performance of their daily work.
- Internet access from the corporate network will be restricted by means of control devices incorporated into the network. The use of other means of connection must be validated in advance and will be subject to the above considerations regarding Internet use.
- Users must not use the name, symbol, logo or symbols similar to those of Grupo Azpiaran in any Internet element (e-mail, web pages, etc.) that is not justified by strictly work-related activities.
- The transfer of data to or from the Internet will only be permitted when related to business activities. The transfer of files not related to these activities (e.g. downloading programmes, multimedia files, etc.) will be prohibited.

#### **4.10. Traceability of system use**

Privileged access will be recorded and these records will be kept in accordance with the Organisation's backup regulations.

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

Errors and failures recorded in system activity shall be analysed, and the necessary measures shall be taken to correct them.

#### **4.11. Identity and access control and management**

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

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

Users must not use any other user's authorised access, even if they have the owner's authorisation.

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

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

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

- Capital letters
- Lowercase letters
- Numbers
- Special characters

It is advisable to use the following guidelines when selecting passwords:

- Do not use well-known words or words that can be associated with yourself, such as your name.
  - The password should not refer to any recognisable concept, object or idea. Therefore, you should avoid using significant dates, days of the week, months of the year, people's names, telephone numbers, etc. in passwords.
  - The password should be virtually impossible to guess. But 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 provider organisation must ensure that it periodically verifies that only duly authorised persons have access to the protected information.

In cases where the Azpiaran Group's information systems are also accessed, the following regulations must also be taken into account:

- No user will receive an access identifier to Grupo Azpiaran's systems until they have accepted the current security regulations in writing.
- Users shall only have authorised access to the data and resources they need to perform their duties.
- If the system does not automatically request it, the user must change the temporary password assigned the first time they log in to the system.
- If the system does not automatically request it, users must change their password at least once every 90 days.
- Temporary authorised accesses shall be configured for a short period of time. Once this period has expired, they shall be deactivated from the systems.
- With regard to personal data, only authorised persons may grant, alter or revoke authorised access to data and resources, in accordance with the criteria established by the person responsible for the file.
- If a user suspects that their authorised access (user ID and password) is being used by another person, they must change their password and report the incident to the Grupo Azpiaran email address.

### **4.12. Change management**

All changes to the ICT infrastructure must be controlled and authorised, ensuring that no uncontrolled components form part of it.

It must be verified that all new components introduced into the ICT infrastructure of the provider organisation used to provide the service function properly and fulfil the purposes for which they were incorporated.

### **4.13. Technical change management**

All changes must be carried out in accordance with a formally established and documented procedure, which ensures that the appropriate steps are followed to implement the change.

The change management procedure must ensure that changes to the ICT infrastructure are minimised 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 adverse or unforeseen side effects on the operation and security of the ICT infrastructure.

Supplier organisations must scan and mitigate any technical vulnerabilities in the infrastructure used to provide the service, informing Grupo Azpiaran of any vulnerabilities associated with critical components.

### **4.14. Security in development**

The entire outsourced software development process will be controlled and supervised by Grupo Azpiaran.

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

The software specifications must expressly contain the security requirements to be met 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.

The internal processes developed by the applications must incorporate all the necessary validations to ensure that no corruption of information occurs.

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

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

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

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

During application testing, it must 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.

With regard to web services, the Owasp Top 10 management will be taken into account.

### **4.15. Contingency management**

The service must have a plan in place to ensure its provision even in the event of contingencies.

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

The provider organisation must be able to demonstrate the viability of the existing contingency plan.

## **5. Monitoring and control**

In order to ensure the correct use of the aforementioned resources, through the formal and technical mechanisms deemed appropriate, Grupo Azpiaran will carry out checks, either periodically or when deemed necessary for specific security or service reasons.