CCN
centro criptológico nacional

ICT Security Guide
CCN-STIC 823

USE OF CLOUD SERVICES

JANUARY 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edit:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.01.26 13:50:11 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-005-X

Date of edition: January 2022
Institute CIES has participated in the production and modification of this document and its annexes.

INDEX

1. INTRODUCTION

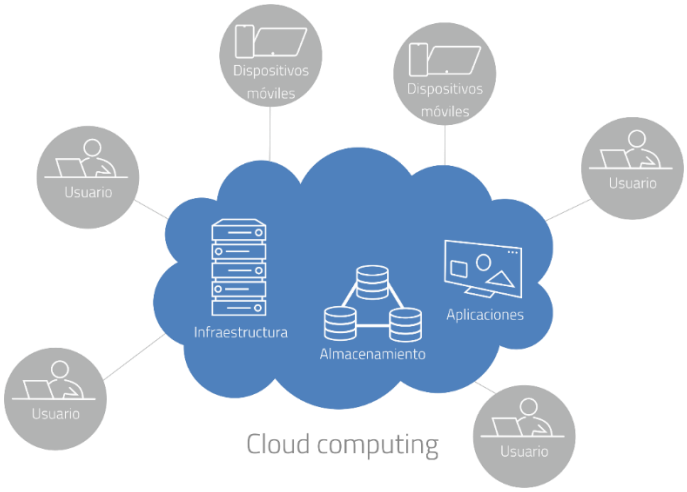
1.1 PREVIOUS CONCEPTS

1. Nowadays, access to online services has increased exponentially. This fact, as well as the heterogeneity of the devices that provide access to these services, has led to a boom in the use of web technologies as a standard.

2. The migration to web environments, the use of mobile applications and the introduction of IoT devices have been a catalyst for the outsourcing of information systems in a large number of organisations. As a result of this situation, the cloud services model emerged as a technological proposal capable of offering a large number of network services in an agile and flexible way, with great possibilities for scalability while minimising deployment times.

3. Cloud services consist of the provision of software, platforms or infrastructures by a provider (CSP, Cloud Service Provider) or by the entity itself, accessible on the network, regardless of where the information systems are hosted and in a transparent manner for the end user.

4. Traditional on-premise systems are no longer as isolated as in the past, presenting a larger area of exposure and blurring the network perimeter. The Cloud allows the use of technologies specifically designed for outsourcing needs by introducing new architectures and security paradigms, which increasingly makes them a secure alternative for processing and storing data.



5. Cloud service provision is a model that enables convenient, on-demand network access to a set of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and deployed and, thanks to automation in the management of services, allows for minimal interaction with the service provider.

6. The cloud services model offers organisations great benefits such as delocalisation, high availability, information accessible from anywhere, low latency, flexibility in resource allocation and significant economic savings, as well

as facilitating new production models such as teleworking, telemedicine or the widespread use of the internet of things.

7. There are different types of cloud services, both in terms of the deployment model (private, public, community or hybrid) and the service categories provided: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS).

8. This guide aims to cover the aspects that should be considered for the adoption of the cloud as a technological paradigm for the provision of services with adequate security guarantees, in accordance with the National Security Scheme (ENS).

1.2 CHARACTERISTICS OF CLOUD SERVICES

9. The main characteristic of the cloud is the accessibility of information. This model, together with the capacity for automatic deployment of services in a matter of seconds at a global level, facilitates access to information by users, regardless of the place or type of device used: it is enough to have access to the network, although the use of this paradigm usually implies the need for connections with significant capacity.

10. Another characteristic that makes the cloud an expanding industry is the economic savings. Generally, the cloud service model allows organisations to reduce costs compared to the traditional service and hosting model. This is due to the savings in resources that are dedicated internally to hardware, maintenance, dedicated staff, supplies, space and facilities, and also due to the use of economies of scale in cloud services, where the greater the need for resources to provide the service, the lower the cost of these resources.

11. In addition, with the cloud service, a customer is allowed to charge only for the resources it uses, either by billing based on parameters such as processor cycles consumed, bandwidth or dedicated virtual machines, or by allowing resources to be added or removed easily and in real time.

12. On the other hand, cloud services are characterised by the delocalisation of data, where the main advantage is that the client can decide the geolocation of the information and allows data and processes to be taken to the most convenient place for the organisation, as well as maintaining access control wherever the data is located.

13. In this way, copies of the server can be maintained in different locations around the globe both to improve access times and minimise latency, and to avoid loss of data or services due to the failure of a processing centre, while maintaining high availability and durability. This offshoring has security implications that organisations should properly assess before making use of cloud services, such as the application of regional data laws or the low availability of network infrastructure in the region, and should apply the security measures and configurations that are appropriate to each scenario.

14. Five (5) essential characteristics are identified for cloud services:

    - **Self-service on demand.** The customer can adjust the required capacity unilaterally, without the need to involve the supplier's staff.
    - **Wide access through networks.** Standard access through networks, enabling all types of access devices: phones, tablets, laptops, personal computers, servers, etc.
    - **Resource aggregation and sharing.** Provider resources are aggregated and made available to multiple customers for sharing. Aggregation includes physical machines and virtual machines that are dynamically allocated on demand. Customers become independent of the physical location of the resources, although locations can be limited to a certain level of abstraction (country, state, etc.) so the can retain control of access to their resources.
    - **Immediate adaptation.** The required capacity can be quickly and elastically provisioned to follow variations in demand. From the consumer's point of view, resources appear unlimited, with any volume available at any time.
    - **Service consumed.** The provider can control the actual service provided at any given time, at the level of abstraction specified by contract, e.g. storage capacity, processing capacity, bandwidth, user accounts, etc. Resource usage can be monitored, controlled and audited, providing great transparency for both the provider and the consumer of the service used.

15. Finally, it is worth noting the possible dependence on third parties for cloud services. The majority trend consists of outsourcing cloud services to third parties, delegating maintenance tasks, system procurement, capacity management, etc..

16. While this is generally seen as an advantage, it should be noted that this outsourcing feature should never lead to a loss of control over information or a disregard for security, as the ultimate responsibility always lies with the contracting agency.

17. When contracting cloud services, it is essential to properly study the conditions of the service and the security measures applied to confirm that they are adequate for the requirements demanded of the client organisation, as well as to establish adequate monitoring and surveillance measures.

1.3 DEPLOYMENT MODELS

18. Given the range of possible deployments when creating cloud services environments, infrastructures can be classified as public, private, community or hybrid.

    - **Public cloud.** The infrastructure of this cloud is maintained and managed by third parties not linked to the organisation, providing resources openly to heterogeneous entities, with no more than a contract with the same provider that controls the infrastructure.

- **Private cloud.** This cloud infrastructure or services provided are fully dedicated to a single customer who controls which applications run and where (on-demand infrastructure). It can be owned, managed and operated by the organisation, a third party, or some combination of these, and can exist on- or off-premises.

  The *public cloud* offers flexibility in terms of contracting, while the *private cloud*, in most cases, requires certain consumption or permanence commitments.

- **Hybrid cloud.** Services are offered publicly and privately. A user owns some parts and shares others, albeit in a controlled manner.

- **Community cloud.** The infrastructure of this cloud or services provided are shared in a closed community by several related organisations that share requirements in order to serve a common function or purpose (security, policy, ...).

  The *community cloud* may be owned, managed and operated by one or more of the community organisations, a third party or some combination of them, and may exist on or off-site.

1.4 SERVICE CATEGORIES

19. A number of service categories are offered, as detailed below:

- **IaaS (Infrastructure as a Service).** It is responsible for delivering an infrastructure to the user, providing processing and storage resources through the network, without any other added value (storage usage services, hardware, servers and network components).

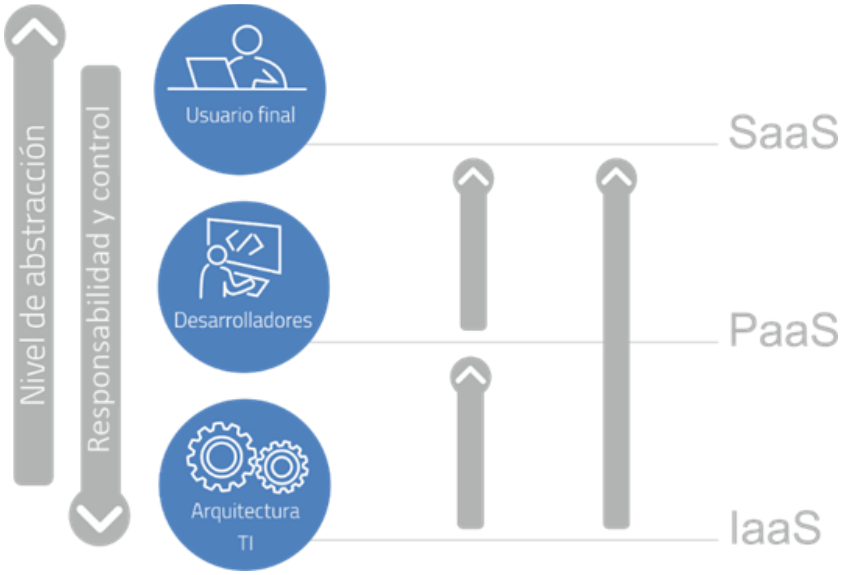
  The provider is responsible for infrastructure management and the customer has control over the operating systems, storage and applications deployed, as well as control over the network components.

- **PaaS (Platform as a Service).** It is responsible for delivering a platform to the client organisation. The customer does not manage or control the infrastructure, but has control over the installed applications and their configuration, and can even install new applications.

  Tools and utilities are provided to develop cloud applications such as databases or programming environments in which the user can develop their own solutions.

- **SaaS (Software as a Service).** A software distribution model in which applications are hosted by a service provider and made available to users through the network.

  The user finds in the cloud the tools with which he can implement the necessary processes: office applications, e-mail, etc... where the client does not manage or control the infrastructure on which the service he uses is based.



1.5 RISKS ASSOCIATED WITH CLOUD SERVICES

20. The adoption of cloud services as a strategy to support information and communication technology (ICT) services offered by different organisations introduces a number of advantages for them, such as cost reduction or flexibility in the incorporation of new resources.

21. However, the adoption of this new technological paradigm introduces new risks that must be controlled in order to provide a service that guarantees the requirements demanded by the legal frameworks, such as the ENS or the current regulations on personal data protection, as well as by the security requirements that organisations establish as necessary in each case.

- **Loss of control.** The customer transfers control to the service provider.
- **Location of data.** It is necessary to agree with the provider that the processing of the data is subject to the legal framework of the country.
- **Regulatory compliance.** Data security and integrity.
- **Data isolation.** The customer transfers control to the service provider.
- **Portability and long-term viability.** Implications for data migration.
- **Privileged user access.** Agreed with the provider for support users.
- **Recovery.** Disaster recovery policy.
- **Monitoring.** Monitoring and surveillance activities are highly dependent on the mechanisms offered by the service provider.

22. In line with the above, compliance with security requirements and how to deal with legal or regulatory compliance differs depending on whether the cloud

infrastructure is owned and managed by a third party or by the organisation itself.

23. In the event that the organisation is the owner and administrator of the infrastructure on which the cloud services are deployed, it is the responsibility of the organisation to ensure full compliance with the regulations in force, while in the event that the infrastructure is operated by a third party, the latter must comply with the requirements established in the security regulations applicable to service providers.

24. In any case, the responsibility for compliance with the ENS or any other applicable rules, as well as for the correct processing of the data in general terms from the point of view of their security, will always lie with the body that owns the information, regardless of the existence of agreements, insurance or other compensatory or complementary monitoring measures.

25. This guide focuses on identifying the requirements that an organisation should consider in order to comply with the ENS by ensuring the security of both information and services provided through the cloud.

2. SAFETY REQUIREMENTS

2.1 FIRST STEPS

26. The body shall categorise the system supported by the cloud solution according to ANNEX I of Royal Decree 3/2010, of 8 January, which regulates the National Security Scheme in the eGovernment field.

    To this end, the following actions will be carried out:

    - **Determination of security levels (LOW, MEDIUM, HIGH, UNVALUED)** required for each of the security dimensions, Availability [D], Authenticity [A], Integrity [I], Confidentiality [C], Traceability [T] of the services and information provided through the cloud, by determining the impact that an incident affecting the security of the information or systems would have on the organisation.

      Assessment to be carried out and formally approved by the respective Heads of Services and Information.

    - **Determination of the category of the system (BASIC, MEDIUM and HIGH) that supports the services and information provided by the cloud**, based

on the maximum rating obtained in one of the dimensions. The person responsible for its performance and formal approval shall be the System Manager.

- **Preparation of the statement of applicability**, by selecting the security measures in ANNEX II of Royal Decree 3/2010, according to the maximum security values obtained in each of the security dimensions and/or according to the category of the system, as the case may be.

  This document must be formally approved by the Security Officer.

- **Conduct an analysis of the risks to which** the services and information supported by the cloud are exposed. If, as a result, additional measures to those already identified are required, they shall be added to the applicability statement.

- **Adhering to a Specific Compliance Profile**, if the cloud has a profile approved by the National Cryptologic Centre, the organisation will be able to adhere to it, and the applicability statement associated with this specific profile will then apply, and its adoption will have to be formally justified.

27. The category of the system supporting the cloud services, as well as any additional measures deemed applicable, shall be propagated to its constituent elements, whether they are owned by the agency, those of a contracted CSP, or those of a subcontracting chain between CSP.

2.2 CONSIDERATIONS FOR SECURITY IMPLEMENTATION

28. Below is an analysis of the security measures of the organisational framework, the operational framework and the protection measures of Annex II of Royal Decree 3/2010.

2.2.1 Organisational aspects

29. The organisation shall have a **security policy** that is known throughout the organisation, describing the mechanisms in place for the ongoing management of security and establishing who is responsible for ensuring compliance. The cloud solution shall be in line with this policy.

30. The use of a cloud solution will require a specific **security policy** to communicate to service users the acceptable use criteria, which will contain, at least, the following aspects:

    - Permitted uses.
    - Type of information that can be used in the service.
    - Prohibited actions.
    - User responsibilities and obligations (e.g. safekeeping of access credentials, etc.).

- Access and use of the service from personal devices (e.g. smartphones, tablets, laptops, etc.).
- Security tools and measures to be used (e.g. encryption of information, backups, etc.).

31. It will also be necessary to document **safety procedures**, identifying the tasks to be performed, as well as those responsible for carrying them out, related, as appropriate, to:

    - IaaS: virtualised network components, operating systems, storage and deployed applications.
    - PaaS: installed applications and their configuration.
    - SaaS: configuration and parameterisation of the application(s) as a service.

32. To the extent that there is capacity for the introduction of new elements in the cloud system, this action will require the definition and implementation in the organization of a **formal authorisation process** to introduce these components into the system, being necessary the identification of the responsibility of each party (agency/CSP).

2.2.2 Operational security aspects

2.2.2.1 System planning

33. For the purpose of **risk analysis**, the organisation shall reflect the assets according to the cloud model:

    - In the case of a SaaS service, the cloud solution will be reflected as an "external services" asset, on which the services and information supported by it will depend.
    - In the case of a PaaS and IaaS service, the assets over which it has control shall be indicated.

34. In the event that services are provided from an on-premise private cloud, the agency shall reflect in the risk analysis all assets involved in the provision of services.

35. The same criterion shall be followed for detailing the elements (equipment, networks, firewalls, etc.) defining the **security architecture**.

36. To the extent that the agency has the capacity to do so, the process of **acquiring new components** for the system in the cloud will require an analysis of whether they are consistent with the defined security architecture, whether they take into account the risks to which the system is exposed and the technical, training and funding requirements.

37. For the **sizing** study and the necessary **capacity**, the following aspects shall be taken into account, depending on the type of cloud, before any new element is put into operation:

- In the case of a SaaS service, measure of the service capacity will be determined by the provider itself, and may be based on the number of registrations, software instances, number of concurrent users or any other measure generally referring to the software functionalities contracted.

  Whatever the scale for determining the capacity of the contracted service, this must be expressly stated in the agreement, as well as the penalties to be adopted in the event that the capacity parameters are not met.

- In the case of a PaaS and IaaS service, it is more common to measure the capacity of the service in terms of CPU cycles, usage time, data transferred, bandwidth or disk storage capacity, and in the case of IaaS it is even possible to require the characteristics of the contracted hardware: disk size, RAM memory, type of processor, CPU or data transfer. The existence of services that allow the use of these capacities to be monitored must be ensured.

38. In any case, regardless of how the capacity of the service is measured, it is necessary to specify the conditions under which the contracted capacity may be modified, either to increase or reduce it, even in real time according to the demand at any given moment.

    The agency shall define and appropriately reflect maximum and minimum values between which the allocation of resources is done automatically or semi-automatically, without the need for substantial modifications to the service agreements with the provider.

39. Finally, the CSP will provide tools or other resources that allow the organisation to measure the capacity of the service and its performance, so that it has reliable data to ensure that in the event of load increases and decreases, the platform has continued to work in accordance with the values agreed.

2.2.2.2 Access control

40. When the organisation has adopted a Specific Compliance Profile, configuration of the measures related to the **access control** to resources shall follow the guidelines described in the configuration guides associated to the corresponding profile.

2.2.2.3 Exploitation

41. For the maintenance of the **asset inventory**, and depending on the cloud model, the following shall be taken into account:

    - In the case of a SaaS service, the cloud solution will be reflected as an "external services" asset.

    - In the case of PaaS and IaaS services, the assets over which they have control shall be reflected. It is possible to make use of inventory tools provided by the provider to complement its own inventory.

42. In the case where services are provided from an on-premise private cloud, the organisation shall reflect in the inventory all assets involved in the provision of the services.

43. In case the organisation adopts a Specific Compliance Profile, the **security configuration** (bastioning) of the equipment will follow the guidelines in the configuration guides for that profile.

44. For the performance of **maintenance** tasks and the **management of changes**, the organisation shall define responsibilities and protocols of action with the CSP, thus preventing unforeseen outages or errors, which could affect the provision of services.

45. The organisation shall have in place a comprehensive procedure for the **management and logging of security incidents**, which also takes into account the obligations imposed by the data protection regulation.

    In this regard, the "**Technical Security Instruction on Security Incident Notification[1]"**, approved by Resolution of 13 April 2018 of the Secretary of State for Public Administration, which establishes that Public Administrations shall notify the National Cryptologic Centre of incidents that have a significant impact on information security and **Article 33 "Notification of a personal data security breach to the supervisory authority"** of EU REGULATION 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

46. This procedure shall include the information flows that have been established with the CSP to ensure smooth communications and compliance with the deadlines established in the management of the incident.

47. The agency shall take into account that the CSP has user **activity logs** that allow monitoring, analysing, investigating and documenting improper or unauthorised actions, both at operational and management level. Therefore, responsibility for the activity logs shall be established with the CSP, establishing obligations regarding their configuration, the periodic consolidation of data, the retention of the logs and regarding the mechanisms implemented for the **protection of activity logs**.

    In the event that the organisation has adopted a Specific Compliance Profile, the provisions of the Application Profile Configuration Guide shall be followed.

[1] Establishes the criteria and procedures for notification by the entities that are part of the subjective areas of application of Law 39/2015, of 1 October, on Common Administrative Procedure for Public Administrations, and Law 40/2015, of 1 October, on the Legal Regime of the Public Sector to the National Cryptologic Centre (CCN) of those incidents that have a significant impact on the security of the information they handle and the services they provide in relation to the category of the system, in order to be able to adequately respond to the mandate of Chapter VII, Response to security incidents, of Royal Decree 3/2010, of 8 January.

48. If cryptographic keys are kept in the CSP's infrastructure, the CSP shall inform the organisation of the measures implemented to **protect the cryptographic keys** throughout their life cycle (generation, transport, custody, withdrawal and destruction). Otherwise, the customer shall be responsible for their safekeeping and protection.

2.2.2.4 Contracting a cloud service provider

49. For the contracting of a CSP, the agency will establish a series of **contractual conditions** in the provision of the service, relating to the characteristics of the service to be provided, the responsibilities of both parties.

    In turn, "service level agreements" will be established to define the quality of the contracted service, as well as the mechanisms to be established for its measurement.

50. In addition, Law 9/2017, of 8 November, on Public Sector Contracts, which transposes into Spanish law the Directives of the European Parliament and Council 2014/23/EU and 2014/24/EU of 26 February 2014, regulating procurement procedures by public administrations, will be taken into account.

    Cloud services fall within the typology of service contracts, in accordance with article 17 of the aforementioned Law. Other necessary aspects regulated by the aforementioned Law would be those relating to the confidentiality of the bidders' information, as well as that of the organisations, regulated in Article 133, and the conditions under which the contractor is acknowledged as the data processor, regulated by the 25th additional provision.

51. Likewise, the CSP must be required to provide systems that comply with the ENS, within the category of the services to be provided through this cloud. This obligation is set out in the "Technical Security Instruction on compliance with the National Security Scheme", approved by Resolution dated 13 October 2016 of the Secretary of State for Public Administrations.

52. **These aspects, as a general rule, shall be regulated prior to contracting, in the specifications and/or tenders requests**. At least the following shall be taken into account:

    - **Service Description**: detailed description of the service to be provided by the provider, including service level agreements and all service specifications.
    - **Type of service and infrastructure**: the type of service and infrastructure to be contracted, as specified in section "1.2 Characteristics of cloud services".
    - **Sizing of the service**: the resources that will make up the service, taking into account what is established in the "Planning" section of this guide.
    - **Service Level Agreements**: agree on the Service Level Agreements (SLA), which will govern the quality of the contracted service, reflecting aspects related to capacity, availability, continuity or incident management, change requests, among others, with at least the following criteria:

- **Capacity**: load deviations to be assumed by the provider will be defined. Similarly, notification times shall be defined when insufficient resources are detected.
- **Availability**: service availability percentages will be established according to the criticality of the service, identifying if there are critical periods in which higher levels of availability are required. Recovery times for information systems shall be defined according to the system category required of the CSP.
- **Change requests and incidents**: response and resolution times shall be defined, as well as the timetable for dealing with change requests made by the client organisation or incidents reported automatically or manually.

For each SLA, the following aspects shall be required to be defined:

- Parameter: SLA identifier.
- Responsibilities: who collects and provides the data necessary to perform the calculations.
- Formula: description of the calculation to obtain the SLA.
- Periodicity of data capture, of the calculation of derived metrics and of the verification of warning and alarm thresholds.
- Thresholds: minimum values in service provision that trigger warning situations (monitoring required) and alarm situations (correction required).
- Penalty: procedure for determining and quantifying the consequences of non-compliance with SLAs.

53. The periodicity of SLA compliance reports and/or mechanisms provided for their measurement shall also be determined.

- **Responsibilities and obligations**: the responsibilities involved in the provision of the service will be defined, both on the side of the contracting body and the CSP: incidents, change management, maintenance, etc.
- **Activity log**: responsibilities for activity logs shall be defined, taking into account the provisions of the "Operation" section of this guide.
- **Incident management**: information flows and those responsible for their management shall be established, taking into account the provisions of the "Operation" section of this guide.
- **Data backup and recovery**: responsibility for data backup and recovery shall be established, taking into account the provisions of the "Asset Protection Measures" section of this guide.

- **Continuity of service**: this shall reflect the measures to be implemented to ensure continuity of operations, taking into account the provisions of the "Continuity" section in this guide.
- **Termination of the contract**: aspects relating to the return of the information will be regulated, in terms of format and deadlines. Or, failing this, aspects relating to the destruction of the information, requiring evidence (certificates) of the same.
- **Information on subcontracting**: obligation to report on subcontractors to prove how they comply with the obligations that have been required of the organisation prior to contracting and which, in turn, are extended to its suppliers and service providers.
- **Legal requirements**: this will include aspects relating to compliance with legal obligations, such as:
  - Apply for **ENS compliance**, in the category corresponding to the systems supporting the services to be provided through this cloud.
  - Regarding **information confidentiality**, whether it be information to which tenderers have access before the contract is awarded, information to which the successful tenderer has access during the performance of the contract, or information provided by the tenderers.
  - Regarding **compliance with current legislation on data protection**: RGPD [2]and LOPDGDD [3].
  - Compliance with the obligations established by **the "Royal Decree-Law 14/2019, of 31 October, adopting urgent measures for reasons of public security in matters of digital administration, public sector procurement and telecommunications"** which, among others, establishes aspects relating to the location in the European Union (EU) of the technical resources used for identification and signature systems based on a concerted key (or similar) or in Spain if these contain special categories of data and also with respect to the location (and provision) in the EU of information and communications systems related to the Register of Inhabitants, population registers, tax management and the national health system.
  - In the event that the object of the contract involves **access to** personal **data**, the PSC acquires the status of data processor and is therefore obliged to comply with the provisions of article 28 of the GDPR, in accordance with the provisions of the section **"Measures for the protection of assets"**.

[2] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)

[3] Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights.

- **Geographical constraints**: conditions may be set on the geographical location of servers and/or communication lines depending on the information (including personal data) to be hosted or transported respectively.

  These conditions, as a general rule, derive from requirements that the organisation itself establishes as necessary or due to legal conditions, established by compliance with the prescriptions on international data transfers outside the EU. of the General Data Protection Regulation and Organic Law 3/2018, of 5 December, on Data Protection and guarantee of digital rights as well as those established in other regulations, criteria or guidelines related to data protection or the "Royal Decree-Law 14/2019, of 31 October, adopting urgent measures for reasons of public security in matters of digital administration, public sector procurement and telecommunications".

54. On the other hand, it will also regulate how the **quality of the service** provided by the CSP is **monitored**, defining the mechanisms that the provider will implement so that the organisation can verify that the agreed service quality levels are met.

    Either through their own technical controls or through the periodic review and approval of service reports provided by the CSP. These reports will detail any significant anomalies or deviations that have occurred during the period, as well as the actions that have been implemented in response to these situations that could pose risks to the organisation.

55. To monitor compliance with data protection regulations, compliance controls can be established either by third parties auditing the CSP, or by submitting evidence of compliance, e.g. audit reports of regulation, confidentiality contracts with staff, etc. Documentation that could be accessible for consultation on the CSP's websites.

56. Sample clauses to be included in tender requests and/or specifications are included in the Annex SAMPLE CLAUSES TO BE INCLUDED IN SPECIFICATIONS AND SERVICE LEVEL AGREEMENTS.

2.2.2.5 Continuity

57. In order to carry out an **impact analysis**, the organisation shall identify the availability requirements that will apply to the services provided by the cloud and shall verify that they correspond to those contracted with the CSP, it will also identify all the elements that are critical for the provision of each service.

58. The continuity of services supported by the cloud solution, required for HIGH category systems, shall be provided by the CSP. The ENS certification of HIGH category by the CSP shall be sufficient evidence of compliance with these requirements. In any case, evidence of compliance with the following security requirements may be required:

- Planning of **alternative means for the provision of services** provided by third parties to those currently contracted.
- Existence of a **continuity plan** with a corresponding **test plan**.
- Provision of **alternative staff** who can take over the tasks of the current staff in case of unavailability.
- Existence and availability of **alternative facilities** in case of unavailability of the usual ones.
- Ensuring the existence of **alternative means of communication** in case the current ones fail.
- Availability of **alternative means available to the CSP to provide the services** in case of failure of the usual ones.

59. In the case the provisioning is made from an on-premise private cloud, the organization will be responsible for its implementation.

2.2.2.6 System monitoring

60. The CSP shall have **intrusion prevention or detection** tools in case the services are supported by an on-premise private cloud, but the organisation will be the one implementing these functionalities.

61. For the collection of the data necessary to know the degree of implementation of security measures, to respond to the National Report on the State of Security, as well as those related to incident management system, indicators and the associated **metrics system** will be defined, also taking into account the data related to the services supported by the cloud.

2.2.3 Asset protection measures

62. Security measures relating to the **protection of facilities and infrastructure** shall be covered by the CSP. In case the provision is made from an on-premise private cloud, the organisation shall be responsible for its implementation.

63. Measures regarding security in **personnel management** (job profiles, awareness, training, roles and duties) will be covered by the CSP in relation to the provision of cloud services, however, these measures will also apply to the organisation in relation to the personnel related to these services.

64. The measures relating to the **protection of equipment** (workstation locking, laptop protection, etc.) will be covered by the CSP for the provision of cloud services, however, these measures will also apply to the organisation for the equipment related to these services.

65. The measures relating to the **protection of communications** (perimeter protection system, confidentiality, integrity and authenticity of communications, network segregation) will be covered by the CSP with regard to the provision of

cloud services; however, these measures will also apply to the organisation with regard to the communications it carries out on these services.

66. Measures relating to the **protection of information support** (labelling, encryption, safekeeping, transport, erasure and destruction) shall be covered by the CSP in relation to the provision of cloud services, however, these measures shall also apply to the organisation in respect of the medium related to these services.

67. The measures relating to the **protection of applications** (secure development, acceptance testing and commissioning) shall be covered by the CSP for the software related to the provision of cloud services, however, this measure shall also apply to the organisation for software of its competence related to the services.

68. In the event that cloud services involve the processing of **personal data**, prior to contracting, it is recommended to follow the recommendations established by the Spanish Data Protection Agency in the "Guide for customers contracting cloud computing services".

69. In this regard, it should be borne in mind that when processing personal data, the CSP is acknowledged as the processor and will therefore be obliged to comply with the provisions of Article 28 of the GDPR, which establishes the need for this processing to be governed by a contract or other legal act under European Union or Member State law, which binds the processor to the data controller and establishes the purpose, duration, nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller.

    Such contract or legal act shall stipulate, in particular, that the controller will be responsible for:

    - processing the data for the stated purposes and in accordance with the instructions of the organisation.
    - The obligation of confidentiality of CSP staff with regard to data.
    - Determining the security measures to be applied. In this point, the provisions of the "First additional provision. Security measures within the scope of the public sector" of the LOPDGDD[4], which establishes that the security measures provided for in the National Security Scheme must be applied to the processing of personal data.
    - Planned disposals.
    - Planned subcontracting.
    - Planned subcontracting regime. Initially planned subcontracting.
    - International data transfers.

[4] Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights.

- International data transfer regime. Planned transfers.
- The existence of the data protection officer (if applicable).
- The location of treatments.
- Register of Processing Activities (RAT), where applicable.
- The processing of the rights of access, rectification, erasure and opposition, limitation of processing, data portability and the right not to be subject to automated individual decision making or other rights recognised by the applicable regulations.
- The management of security breaches, aligned with that established for the management of security incidents. Regulation of the communication and/or notification of security breaches, deadlines, means and evidence.
- Collaboration regime with the Controller in other obligations: preparation of Privacy Impact Assessments relating to the protection of personal data (DPIA), analysis of associated risks, etc.
- Regulation of due diligence measures required of the provider, including possible audits and/or supervisory checks on compliance with data protection regulation.
- Responsibility regarding the right to information on the collection of personal data by service users.
- Regulation of the restitution of personal data, aligned with the conditions set out in the contract termination.

70. In the event that the provision of services is carried out from a private cloud "on premise", the organisation shall be responsible for compliance with data protection regulations, except in those aspects associated with the maintenance service and/or incident support services or developments or security patches, when this involves access to personal data of the Data Controller.

71. In case the CSP provides mechanisms that allow the labelling of information hosted in the cloud, the organisation may align its **information rating** procedure with it.

72. The process of **cleaning documents**, removing from them unneeded information contained in hidden fields and/or metadata shall be the responsibility of the organization owning the documents managed by the cloud services.

73. Where the CSP is responsible for **backups**, the organisation shall request information from the CSP on the backup procedure and backup tests implemented, at least on the following aspects:

- Scope of backups.
- Backup policy.
- Encryption measures for backup information.

- Procedure for requesting backup restorations.
- Performance of restoration tests.
- Transfer of backups (if applicable).

2.2.3.1 Protection of services

74. The implementation of measures for the **protection of e-mail** threats shall be the responsibility of the organisation, unless the CSP provides the e-mail service.

75. The implementation of measures for the **protection of web services and applications** from threats inherent to this medium will be covered by the CSP with regard to the provision of cloud services in the SaaS mode, otherwise it will be the responsibility of the organisation.

76. Measures related to the **protection against denial of service** will be implemented by the CSP, unless service provision is done from a private cloud "on premise", being then the responsibility of the organisation.

2.2.3.2 Audit

77. If the services are provided from a system supported by an on-premise private cloud, with HIGH-category, the **cloud service shall be required to have successfully passed a penetration test audit (pentesting)** by an independent third party to assess the security maturity of the service and to identify potential vulnerabilities in the service.

    This audit will check the absence of public vulnerabilities that could compromise the information handled or the service provided.

78. In the event that the cloud service is a security service, this third party must be an independent laboratory accredited by the National Accreditation Entity (ENAC), following evaluation methodologies recognised by the CCN's Certification Body of the National Scheme for the Evaluation and Certification of Information Technology Security (ENECSTI).

2.2.3.3 Transparency

79. The service provider must be able to:

    - Provide visibility to the customer of the security tools available to them, including those for monitoring, analysing, recovering and reporting security incidents.
    - Inform the user of the type of virtualisation used and the level and mechanisms of segregation of their data or applications hosted in the cloud.
    - Inform the user of the mechanisms and procedures for secure deletion of the information stored by the provider, which will be used at the time of termination of the contractual relationship.

2.2.3.4 Registration information

80. Allow the customer to access and analyse the different logs, access records and any other information that may be requested to ensure compliance with legal obligations.

    In case of security incidents, all required information (configuration, logs, etc.) of physical equipment, network devices, shared services and security devices must be provided to the customer.

2.2.3.5 Encryption and key management

81. The service shall have **encryption mechanisms** for the protection of user information, in transit and at rest, so that it cannot be read or modified in the event of illegitimate access. The cryptographic mechanisms shall comply with the relevant CCN-STIC series guide.

82. The supplier shall comply with one of the following cases:

    - Being able to guarantee the operation of encryption mechanisms without the keys being stored in the cloud. These will be at the disposal of the client, who is responsible for their management and storage.
    - Store the encryption keys in hardware security modules called HSM (Hardware Security Modules) devices, which are not accessible by third parties. These devices must be qualified by the CCN and included in the CCN's Catalogue of Information and Communication Technology Security Products (CPSTIC).

2.2.3.6 Jurisdiction of data

83. The provider shall inform the customer about the **geographical location of its data** (including backups and log storage), before and during the provision of the service.

84. With regard to the geographical limitations of the data, the provisions of Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016, Organic Law 3/2018 of 5 December and Royal Decree-Law 14/2019 of 31 October adopting urgent measures for reasons of public security in the areas of digital administration, public sector procurement and telecommunications, as well as other applicable legislation, shall apply, without prejudice to the requirements established in this Royal Decree.

3. CONCLUSIONS

85. Prior to contracting, it is necessary to identify the **security requirements to be requested from the CSP**, to be included in the contractual conditions, for example:

    - That the system supporting the services contracted has **ENS compliance**, in the category equal to or higher than the one we have determined in the categorisation process.

- Including any **additional security measures** that have been identified as necessary, such as the existence of a continuity plan, when not required by the categorisation of the system (HIGH).
- Defines the **responsibilities and obligations (CSP/organisation)** regarding the implementation of measures, through the detailed analysis of the applicability statement identifying those that are the sole or shared responsibility of the CSP.
- Establishes the quality levels of the services to be contracted, through the establishment of **Service Level Agreements (SLA)** on capacity, availability, changes, etc.
- It establishes the **necessary legal requirements**, those relating to data protection regulations, confidentiality, geographical location of data, etc.
- Possibility of **using a Specific Compliance Profile**, which makes it possible to implement the necessary security measures adapted to the cloud, as well as to have configuration guides.
- It includes any other aspect reflected in this Guide.

4. DECALOGUE

	Decalogue of recommendations for the use of cloud services
1	Determine the category of the system (BASIC, MEDIUM or HIGH) that will support the cloud solution, according to ANNEX I of Royal Decree 3/2010.
2	Draw up the applicability statement, according to ANNEX II of Royal Decree 3/2010.
3	Conduct a risk analysis, to identify additional safety requirements, to be reflected in the statement of applicability.
4	Adhere to a Specific Compliance Profile (where applicable).
5	Establish the contractual conditions, prior to contracting, in the tender specifications and/or requests.
6	In the contractual conditions, in addition to those regarding compliance with legal requirements, detail aspects relating to the service, its infrastructure, dimensioning, activity logs, incident management, backups, etc. and establish conditions relating to the termination of the service.
7	Supervise the CSP's compliance with the legal requirements set out in the terms and conditions of contract.
8	Regularly monitor compliance with the Service Level Agreements (SLAs) established with the CSP.

9	Plan regular reviews of information, which the CSP provides through various mechanisms, e.g. activity logs, capacity, storage, etc.
10	Develop a specific security policy for cloud users.

5. ANNEX I Clauses and Service Level Agreements

5.1 Compliance with the National Security Scheme (NSS)

Note: In case of procurement of cloud services through an intermediary entity acting as a service provider (TENDERING or AWARDING ENTITY), but which does not own the systems that will provide the cloud services, it will be necessary to also require ENS compliance to the end systems providing the cloud services, owned by the end cloud service provider.

Considering the provisions of Article 29 of Royal Decree 3/2010, of 8 January, which regulates the National Security Scheme in the field of Electronic Administration, and the Resolution of 13 October 2016, of the Secretary of State for Public Administrations, which approves the Technical Instruction on Security in accordance with the National Security Scheme, which describes the obligation to require private sector operators providing services or solutions to public entities, In accordance with the National Security Scheme, the CONTRACTING ENTITY deems necessary that the suppliers participating in the tender in question shall exhibit the corresponding Statement of Conformity with the National Security Scheme (when the system category is BASIC), or the Certification of Conformity with the National Security Scheme (when the category is MEDIUM or HIGH).

Therefore, based on the above, and on the analysis of risks to which the services subject to the tender are exposed, the CONTRACTING ENTITY, establishes as necessary that the TENDERING ENTITY shall have the corresponding Statement or Certification of Compliance with the National Security Scheme, according to the relevant category of security, of the systems involved in the provision of the services indicated, and it should maintain the compliance in force during the term of the contract. In the event that the successful tenderer is unable to maintain compliance with the NSS - due to loss, withdrawal or suspension of the Compliance Certification or impossibility of maintaining the Compliance Declaration - it must communicate this circumstance immediately and without undue delay to the CONTRACTING ENTITY, which will consider the impact of this circumstance on the provision of the services covered by the contract.

When the contract covers, totally or partially, the use of on-premise systems (e.g. software), in accordance with the provisions of *the CCN-STIC Guide 858 Implementation of SaaS systems in local mode (on-premise*), the TENDERING ENTITY must provide the following documents: Installation Guide (addressed to administrators), the Secure Use Guide (addressed to users) and the Supplier-Customer Relationship Guide.

The AWARDEE assumes its obligation to comply fully with the National Security Scheme, and with the need for the information systems of those suppliers that are essential for the provision of the service covered by the contract to comply with Royal Decree 3/2010 of 8 January.

5.2 Confidentiality clauses

5.2.1 Recruitment confidentiality

Without prejudice to the provisions of Law 19/2013, of 9 December, on transparency, access to public information and good governance, and the provisions contained in Law 9/2017, of 8 November, on Public Sector Contracts, relating to the obligation to publicise the award and to the information to be given to candidates and tenderers, the contracting authorities shall not disclose the information provided by the TENDERING ENTITIES that has been designated as confidential by the latter when they submited their tender.

Confidentiality may concern, inter alia, technical or commercial secrets, confidential aspects of tenders and any other information the content of which could be used to distort competition, whether in the tendering procedure in question or in subsequent tendering procedures.

The obligation of confidentiality may not prevent the public disclosure of non-confidential parts of the contract, such as the settlement, the final deadlines for performance of the services, the identity of the successful tenderer or the essential parts of the tender, as well as subsequent modifications.

Likewise, all the documentation or information provided by the CONTRACTING ENTITY to the tenderers so that they have the information required to submit their corresponding offer is confidential and must be treated as such.

Once the contract is awarded, if the CONTRACTING ENTITY provides the AWARDEE ENTITY with additional information necessary for the provision of the services, such information shall be treated as confidential and shall be treated as such by the AWARDEE ENTITY and by any person involved in or related to the performance of the contract.

When the information submitted includes personal data, it will be necessary to consider the provisions in relation to Data Protection established in the regulations in force.

All persons involved in any stage of the tender process shall be subject to the duty of confidentiality referred to in Article 5.1.f) of the General Data Protection Regulation (EU) 2016/679 (GDPR).

All information processed, generated or relating to the execution of the contract must be processed in accordance with the provisions of the corresponding Tender Document and described in the section that regulates the processing of personal data on behalf of third parties. Otherwise, if no personal data processing is declared or it does not exist, the AWARDEE ENTITY entity shall return all the information to the CONTRACTING ENTITY or its designee at the end of the contract.

5.2.2 Confidentiality in the execution of the contract

The objective and temporary extension of the duty of confidentiality imposed on the AWARDEE ENTITY is determined in accordance with the provisions of Article 35.1.m) of Law 9/2017, of 8 November, on Public Sector Contracts. Therefore, the AWARDEE shall

be obliged to maintain full confidentiality and secrecy with respect to the information handled during the execution of the contract for 5 years from the date of knowledge of the information concerned, unless a different period is determined in the corresponding Tender Documents or in the subsequent contract.

For all purposes, "all information and documentation relating to the CONTRACTING ENTITY, as well as good internal uses, practices and procedures", which may come to the attention of the AWARDEE ENTITY in the performance of the contract, shall be considered confidential. The CONTRACTING ENTITY does not grant any rights to the AWARDEE ENTITY for access to its information system. In the same vein, confidentiality is granted to any information to which it has access during the execution of the contract, which has been given this status in the specifications or in the contract, or which by its very nature must be treated as such, including, expressly, all information associated with security and protection measures, developed configurations, service and application protections, elements and descriptions of infrastructure and architecture, authentication processes and security protocols, communications, incidents, third party reports, capacity controls and evaluations of the availabilities involved, automatic analyses, networks and perimeter protections, elements assigned to continuity, activity logs and associated protections, backup and restoration protocols, maintenance elements and guarantees involved, and any other elements that may be considered a risk for the purposes of the contracted service or the information linked to the same.

The AWARDEE ENTITY undertakes not to disclose, transfer or expose the information owned by the CONTRACTING ENTITY without its prior express written consent. Furthermore, the AWARDEE shall refrain from using the documentation and/or information known or provided during the execution of the contract for purposes other than the execution of the contract.

When the contract does not require access to the CONTRACTING ENTITY's information system but involves access to the facilities, the AWARDEE undertakes to maintain full confidentiality of the information that could be accidentally obtained through access to the facilities, and especially that which could pose a risk to the CONTRACTING ENTITY in case it becomes known and/or could lead to a breach of security.

When the information submitted includes personal data, it will be necessary to consider the provisions in relation to Data Protection, in the regulations in force and stated in the corresponding Tender Document. In the event that the procurement involves access by the AWARDEE ENTITY to personal data for whose processing the CONTRACTING ENTITY is responsible, the AWARDEE ENTITY and all persons involved in any phase of the procurement process shall be subject to the duty of confidentiality referred to in Article 5.1.f) of the General Data Protection Regulation (EU) 2016/679 (GDPR) and stated in this Tender Document. The AWARDEE ENTITY undertakes to enter into confidentiality agreements with the personnel assigned to the performance of the contract, and to maintain constant awareness and training.

5.3 Applicable data protection legislation

If the purpose of the service contained in the contract subject to tender requires the processing of personal data, the provisions of the General Data Protection Regulation (EU) 2016/679 (RGPD), in the Organic Law 3/2018, of 5 December, on Personal Data Protection and guarantee of digital rights (LOPDGDD) shall be met- with special incidence to the provisions of its First Additional Provision - and the remaining applicable regulations, as well as, where applicable, the provisions of Royal Decree-Law 14/2019, of 31 October, which adopts urgent measures for reasons of public security in matters of digital administration, public sector procurement and telecommunications, which shall be applicable to the AWARDEE ENTITY and its possible subcontractors, throughout the duration of the contract, regardless of the location of the systems involved in the provision of the services.

The purpose of the processing of personal data by the CONTRACTING ENTITY shall be to provide the services covered by the contract. The use of personal data for purposes other than those stated above shall constitute a breach by the AWARDEE ENTITY, which may result in the termination of the contract.

5.4 Declaration of location

As established in Law 9/2017, of 8 November, on Public Sector Contracts, considering the nature of the service, the AWARDEE ENTITY shall provide the identification of the location of the information systems linked to the services covered by the contract, including all the locations associated with the storage and provision of the service, contemplating all the activities involved, such as collection, storage, processing and management.

The AWARDEE ENTITY must identify all subcontractors that will participate in the performance of the services covered by the tender, both in the tender submitted and during the term of the contract, and must identify the location and the specific services provided by each of them. Subcontracting shall in all cases be subject to the provisions contained in the data protection regulations, without exception.

For all purposes, the limitations established in the data protection regulations relating to international data transfers shall be considered. Compliance with such provisions is an essential condition, which shall be extended to the subcontracted entities. This obligation is considered essential to the contract and shall be maintained throughout the term of the contract.

Any modification during the course of the contract relating to the requirements set out in this paragraph must be communicated without delay to the CONTRACTING ENTITY.

5.5 International Data Transfer

No transfers shall be made to a third country or international organisation outside the European Union, except in the cases specifically authorised by the General Data Protection Regulation (EU) 2016/679 (GDPR) and Organic Law 3/2018, of 5 December,

on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), the only exception being the transfer to countries, organisations or territories that have been declared to have an adequate level of protection by the data protection supervisory authorities, or when the transfer is necessary in compliance with a legal obligation, international agreement or court order.

The AWARDEE ENTITY shall communicate without undue delay any change in relation to the conditions for the transfer of personal data, especially the loss of the "adequate level of protection" for international transfers, in accordance with the GDPR. This expressly includes cases in which the Commission determines the loss of the adequacy of a country, organisation, entity or company, including those that no longer adhere to any international agreements that allow international data transfers.

5.6 Service associated with electronic identity verification

Considering the provisions of Law 39/2015, of 1 October, on the Legal Regime of the Public Sector, and in the event that the service tendered by the CONTRACTING ENTITY includes a system of identification by means of an agreed password for the purposes described in Article 9.2c) of the aforementioned law, it shall be necessary that the bids submitted by the TENDERING ENTITIES include or facilitate the identification of the location and provision of the service, as well as the technical resources that are going to be assigned for the collection, storage, treatment and management, which may only be located in the territory of the European Union, in accordance with the provisions of Article 122.2c) of Law 9/2017, of 8 November on Public Sector Contracts. Where special categories of data are involved, as provided for in article 9 of the General Data Protection Regulation (EU) 2016/679 (GDPR), the location shall be limited to the national territory.

To all intents and purposes, when the service tendered allows subcontracting, this shall be subject to the same terms as described above. Therefore, it will be necessary to expressly declare the location of the services or resources concerning the subcontracted processes. When there are several subcontractors, it will be necessary to declare this for each of them individually.

When the contract has already been awarded, and there is a modification that affects the location or provision of the service, including changes in subcontracting, the CONTRACTING ENTITY must be notified without delay, clearly identifying the changes made. This entitles the CONTRACTING ENTITY to terminate the contract.

The AWARDEE ENTITY shall in all respects be directly liable for any failure to comply with the subcontracting and for the declared obligations.

5.7 Processing of data of the types described in Article 46 bis of Law 40/2015

Considering the provisions of Article 46 bis of Law 40/2015, of 1 October, on the Legal Regime of the Public Sector and in cases where the service tendered by the CONTRACTING ENTITY affects data relating to the electoral roll, municipal registers of

inhabitants and other population registers, tax data related to own or assigned taxes and data of users of the National Health System, it will be necessary for the TENDERING ENTITIES to include in their offers the location and provision of the service, which may only be provided within the territory of the European Union.

To all intents and purposes, when the service tendered allows subcontracting, this shall be subject to the same terms as described above. Therefore, it will be necessary to expressly declare the location of the services or resources concerning the subcontracted processes. When there are several subcontractors, it will be necessary to declare this for each of them individually.

When the contract has been awarded, and there is a modification that affects the location or provision of the service, including changes in subcontracting, the CONTRACTING ENTITY must be notified without delay, clearly identifying the changes produced, being the CONTRACTING ENTITY entitled to terminate the contract.

The AWARDEE ENTITY shall in all respects be directly liable for any failure to comply with the subcontracting and for the declared obligations.

5.8 Contract termination regulation: Technology transfer

During the execution of the contract, the AWARDEE ENTITY undertakes to provide the persons designated by the CONTRACTING ENTITY with all the information and documentation requested by them in order to have full technical knowledge of the circumstances in which the services are developed, their activities and, in general, all the technical operations, as well as possible problems that may arise and the technologies, methods and tools used to solve them.

After the end of the contract, the CONTRACTING ENTITY shall develop the necessary actions for the transfer of the knowledge and information involved in the service. The process shall include, necessarily and at the request of the CONTRACTING ENTITY, the return of all the information to the CONTRACTING ENTITY itself or to whoever is designated by it, within a maximum period that will be determined in the corresponding Tender Document, by means of the necessary secure means and the information must be in a format that will be determined in the corresponding Tender Document.

For the technology transfer and restitution process, the successful AWARDEE ENTITY shall submit a detailed plan, including the means to be used, the contingency actions designed and the risks that may arise in the process. When necessary, and especially when there is a new awardee entity, the transition period for the organised management of the transfer and restitution process shall be included.

For the purposes of compliance with current data protection regulations, the legal retention periods that may be mandatory for the awardee entity shall be taken into account.

This clause will be mandatory when the service is terminated early, with the outgoing awardee being responsible for an orderly transfer and restitution.

5.9 Management of data backup and restoration

The AWARDEE ENTITY shall have the necessary mechanisms in place to implement a backup and recovery testing policy that includes at least the following requirements:

- Identification of the scope of backups.
- Backup policy.
- Encryption measures for backup information.
- Procedure for requesting backup restorations.
- Carrying out restoration tests.
- Transfer of backups (if applicable).

5.10 Disaster recovery management (continuity plan)

To ensure the continuity of the services covered by the contract, the AWARDEE ENTITY shall have and submit a contingency recovery plan. This plan shall be activated in the event of total or partial unavailability of the main resources, which for any reason causes the unavailability of the services covered by the contract. This plan shall include:

- Identification and description of planned alternative means of service provision, alternative personnel, existence or planning of alternative facilities and means of communication, etc.
- At least one recovery test per year. The final test report must be sent to the person in charge determined by the CONTRACTING ENTITY, as well as a work plan with corrective actions if events or actions to be corrected are detected.
- Updating disaster recovery plan documentation as necessary.

5.11 Standard Service Level Agreement

5.11.1 Scope of services

Without prejudice to the provisions of the corresponding Technical Specifications, the AWARDEE ENTITY shall include in its tender the planned timetable for the provision of the service covered by the contract (e.g. "24 hours a day, 365 days a year", etc.).

In the service level agreement section, the accepted range for each of the indicators described above shall be established, with the exception of the ranges established for maintenance windows.

5.11.2 Communications and incidents

All communications related to the services or to the corresponding Service Level Agreement shall be made by the areas or departments of the CONTRACTING ENTITY declared for that purpose in the corresponding Tender Document.

The tender documents shall also indicate the medium to be used for communications (e.g. e-mail and/or telephone calls, etc.).

It is mandatory that the service provided by the CONTRACTING ENTITY has an operational record of the requests or notifications made by the CONTRACTING ENTITY, using, where appropriate, the tool indicated in the corresponding Tender Documents. For all purposes, this record shall also register incidents and requests, and shall comply with the provisions of the data protection regulations.

5.11.3 Required Service Levels

5.11.3.1 Availability of contracted services

The AWARDEE ENTITY shall provide the following information in its tender:

Indicator 1: ensure availability of contracted services.

Indicator description: percentage of time that services have been active and providing service.

Unit of measurement: percentage.

Metric: I1= Tp-Tc/Tp*100.

- **Tc:** Total time, measured in minutes, that services are out of service during the measured period.
- **Tp:** Total time, measured in minutes, of the measured period.

Minimum frequency of analyses: monthly.

Target value: > 99,5 %.

Penalty: 1.3% of the billing for that period.

5.11.3.2 Availability of contracted services (special conditions)

Indicator 3: guarantee the availability of the contracted services in a certain time slot, e.g. daytime hours 07:00 to 22:00.

Indicator description: percentage of availability of services during daytime hours (07:00 to 22:00 hours) during the measured period.

Unit of measurement: percentage.

Metric: I3= 900-Tc/900*100.

- **Tc:** Total time, measured in minutes, in which services are out of service during the measured period from 07:00 to 22:00 hours.

Minimum frequency of analyses: monthly.

Target value: > 98 %.

Penalty: 1.3% of the billing for that period.

5.11.3.3 Storage availability

Indicator 4: Ensure availability of storage.

Indicator description: percentage of time the storage has been active and providing service.

Unit of measurement: percentage.

Metric: I4= Tp-Tc/Tp*100.

- **Tc:** Total time, measured in minutes, that the storage is out of service during the measured period.
- **Tp:** Total time, measured in minutes, of the measured period.

Minimum frequency of analyses: monthly.

Target value: > 99,5 %.

Penalty: 2.5% of the billing for the period.

5.11.3.4 Troubleshooting, problem solving

Indicator 5: maximise the number of incidents, problems solved.

Indicator description: percentage of incidents, problems accepted and solved.

Unit of measurement: percentage.

Metric: I5= Nr/Nt*100.

- **Tr:** number of incidents, problems solved during the measurement period
- **Tp:** total number of incidents, problems that were open at the beginning of the measurement period plus those that were opened during the measurement period.

Minimum frequency of analyses: monthly.

Target value: > 95 %.

Penalty: 3.2% of the billing for the period.

Incidents and service requests shall maintain a flow with the notifier and shall be closed when they have been communicated to the notifier and no further action is considered.

It will necessarily be included in the register:

- Time at which the incident starts and ends (including the time at which the incident occurs, the time at which it is reported and the time at which the resolution is completed).
- Start reporting time and end reporting time.
- Resolution times.
- Conclusions and improvement.

In this regard, the points required by the applicable regulations for the identification, management and registration of incidents that may affect the

service, which will be agreed with the CONTRACTING ENTITY, will be taken into account.

The AWARDEE ENTITY shall resolve incidents that are properly reported in a given time, as defined in the corresponding tender documents:

- Critical incidence: (For example: 1 working hour or 4 non-working hours).
- Major incident: (For example: 2 working hours or 12 non-working hours).
- Minor incidence: (For example: 3 working hours or 72 non-working hours).

Data will be collected to assess the incident management system, allowing to know the number of security incidents handled (and specifically):

- Time taken to close 50% of incidents.
- Time taken to close 90% of incidents.

Annually, these values shall be collected in a report submitted to the CONTRACTING ENTITY.

5.11.3.5 Resolution of requests for changes and/or updates

Indicator 6: Encourage the correct implementation of changes and/or updates.

Indicator description: percentage of hardware/software installations, changes and upgrades successfully executed and with a maximum resolution time of 2 days.

Unit of measurement: percentage.

Metric: I6= Nr/Nt*100

- **Nr:** number of changes and/or updates correctly executed and with a maximum resolution time of 2 days during the measurement period.
- **Tp:** of changes and/or updates during the measurement period.

Minimum frequency of analyses: monthly.

Target value: > 99 %.

Penalty: 4.5% of the billing for the period.

The necessary tests will be scheduled and, where appropriate, after agreement with the CONTRACTING ENTITY, generating the least possible impact on the operation of the service. All technical stops of the service shall be at times previously agreed with the CONTRACTING ENTITY.

5.11.3.6 Availability of backups

Indicator 7: Ensure availability of backups.

Indicator description: percentage of planned backups that have been successfully executed.

Unit of measurement: percentage.

Metric: I7= Np-Nf/Np*100.

- **Nf:** number of backups planned and not successfully completed during the measured period.
- **Np:** number of planned backups during the measured period.

Minimum frequency of analyses: monthly.

Target value: > 99,9 %.

Penalty: 2.5% of the billing for the period.

5.11.3.7 Reliability of data recovery

Indicator 8: ensure the reliability of data recovery.

Indicator description: percentage of data recovery from successfully executed backups.

Unit of measurement: percentage.

Metric: I8= Nr/Nt*100.

- **Nr:** Number of backup restores successfully completed during the measured period.
- **Np:** number of restores from backups requested during the measured period.

Minimum frequency of analyses: monthly.

Target value: > 99 %.

Penalty: 2.5% of the billing for the period.

5.11.3.8 Activation of the backup service

Indicator 9: ensure a maximum activation time of the back-up service for the indicated services.

Indicator description: time consumed in starting up the backup service.

Unit of measurement: time measured in hours.

Metric: I9= Ta.

- **Ta:** time measured in hours, spent in preparing the backup service to provide a correct service, during the measured period.

Minimum frequency of analyses: monthly.

Target value: < 24.

Penalty: 2.4% of the billing for that period.

5.11.3.9 Availability of contracted capacity

Indicator I10: manage contracted capacity.

Indicator description: to ensure that the contracted capacity thresholds are not exceeded, establishing a threshold at which it will be necessary for the AWARDEE

ENTITY to notify the CONTRACTING ENTITY in order to authorise the increase in resources.

Unit of measurement: time measured in days.

Metric: I10= Ta.

- **Ta:** time measured in days to report that the 85% threshold in usage of contracted resources has been exceeded, during the measured period.

Minimum frequency of analyses: monthly.

Target value: <= 30.

Penalty: 2.5% of the billing for that period.

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL