NOVA IMS Information Management School

MGI

Mestrado em Gestão de Informação
Master Program in Information Management

AUDITING MODELS OF CLOUD COMPUTING SERVICE FOR PUBLIC ADMINISTRATIONS

Sergi Serra Aloy

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School

Instituto Superior de Estatística e Gestão de Informação

Universidade Nova de Lisboa

AUDITING MODELS OF CLOUD COMPUTING SERVICE FOR PUBLIC ORGANIZATIONS

by

Sergi Serra Aloy

Dissertation report presented as a partial requirement for obtaining the master's degree in Information Management, with a specialization in Information Systems Management.

Advisor: Vitor dos Santos Duarte

October 2021

ACKNOWLEDGEMENTS

First, I would like to thank my thesis advisor, Professor Doctor Vítor Duarte dos Santos for his availability, patience and support. His enthusiasm has encouraged me to keep working and focusing for the thesis.

Finally, I would like to thank the participants on the process. Juan Payeras and José Ramón for collaborating.

ABSTRACT

The following dissertation discussion focuses on the Cloud Computing parading into Public Administrations, aiming to establish a process based on ISO/IEC standards to secure the interoperability of the clouds. However, global digitalization grows exponentially and seems to be constrained by legislative and lack of defined structure to achieve integrity between systems and processes to equate on the same level the communications between administrations. One of the main challenges that citizens and governments face, is the portability of sensitive information, by approaching them, both can save lots of bureaucracy and agile data management. In line manner, the economic impact and digital wealth of the citizens can largely improve by addressing a solid model reference model to exchange and send information. As such, the potential of a dynamic interaction between clouds is key for the technological future of the administrations and many institutions have already started to incentivize cloud computing to enable economic, social, and health services opportunities.

KEYWORDS

Cloud Computing, Information Systems, General Data Protection Regulation, Could Governance, Personally Identifiable Information, Service Level Agreement.

INDEX

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

IS	Information Systems
G2B	Government to business
EU	European Union
CC	Cloud Computing
GDPR	General Data Protection Regulation
NIST	National Institute of Standards Technology
IT	Information Technology
SLA	Service Level Agreement
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
CSA	Cloud Services Agreement
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
ICT	Information and Communication Technologies.
OLA	Operational Level Agreement.
C2C	Cloud to Cloud.
DSR	Design Science Research
COBIT	Control Objectives for Information and Related Technology
ITIL	Information Technology Infrastructure Library
SOAP	Simple Object Access Protocol
REST	Representational State Transfer
PII	Personally Identifiable Information
TLS	Transport Layer Security
SSL	Secure Socket Layer

1. INTRODUCTION

While the internet has a lot to offer, public entities have been always slow and rough for digital transformation and its applications. Worldwide governments attempt to deliver economically; social and security growth relies upon ongoing digital.

This research is a comprehensive effort to assess the integrity of cloud computing into administrations and how this powerful tool can contribute to enhancing current systems and benefit the users while interacting with different clouds.

1.1. BACKGROUND AND PROBLEM IDENTIFICATION

It is well known that cloud computing is a tool that offers on-demand services, even though there's a lack of consistency about how to define and interoperate with these services within public administrations (Marek Moravik, 2018). Most of these organizations use their specifications that can impact the interoperability and interactions of the users when there are changing cloud domains or cloud services.

Public services have developed their intranet structures to step ahead in the digital transformation age and align their services with the technology available in the market (Bernard Le Masson, 2014).

Therefore, consolidating public administration within public and private services means that both will have to play with the same game rules, so they interoperate without getting in conflict due to their interactions. From this perspective, open standards are key to a large amount of active work for developing a public organization's Cloud.

Since smart cities are a cluster for these new technologies that combine the public and private sector (Smart Cities, 2017), the analysis of the protocols, interoperability, and responsibilities between the cloud administration, public organization, and the cloud provider must follow a logic defined on their initial agreement, in other words, the use of public sector information by a business (government-to-business – G2B – data sharing) has to be regulated (European Commission, Communication from the commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions, 2020).

"Cloud computing has developed fast and has become crucial for the European data economy. With the Regulation on the free flow of non-personal data, companies are now able to store and process their data in a cloud anywhere on the EU territory. Cloud computing also unlocks access to future and emerging technologies, such as artificial intelligence, high-performance computing, the Internet of Things, and Blockchain" (European Commission, Shaping Europe's digital future, 2020).

Therefore, Cloud Computing (CC) has become a relevant subject that has to be modeled, studied by public institutions to standardize, and explore the applications of this new digital and cloud transformation to enhance the quality and services provided to citizens and enterprises.

Moreover, the General Data Protection Regulation (GDPR) has already set up a precedent on personal data treatment in the public and private sectors. This is an example of standardization for all of Europe since this regulates indifferently of the European Union country how the information must be protected and processed to guarantee the protection of natural persons concerning the processing of personal data as a fundamental right.

Article 8 (1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her (GDPR, 2016).

The European Union (EU) has already started different programs to standardize Cloud Computing (CC) services. The Cloud Select Industry Group (C-Sig) and the European Commission Expert Group on Cloud Computing Contracts; both are clusters created to address the Cloud Computing standardization to harmonize and suggest behavior policies for the CC environment to offer unified services and keep user data privacy.

Cloud computing is a new way of offering services (Sean Carlin, 2012), taking into consideration business and economic models for providing, consuming information.

Nowadays, administrations use to be robust in changing their processes due to the complexity and sensible information they deal with. Meanwhile, Cloud Computing (CC) has been subject to tackle by governments to agile some of the administration processes and transform the current paradigm into a new digital administration. (Bernard Le Masson, 2014).

European Union has started to take its first steps on CC administration by defining a group of public and private clusters to guide and establish the logic and best practices about how European institutions and Governments should approach the use of public cloud (Marek Moravik, 2018).

The opportunities and benefits of cloud computing are noticeable compared to data warehouse storage, this will open future applications that require new standards and interoperability logic between cloud providers, institutions, and final users.

However, we don´t have a solid model of cloud computing service for public entities, reliable and comparable to private companies. Also, there are not many models that are capable to accept quick partibilities from other clouds neither to be compatible with some kinds of data that a public entity could require from different public clouds.

1.2. STUDY OBJECTIVE

This research paper has the main objective to propose a solid model of cloud computing service for public entities, reliable and comparable using auditing techniques. To do so, this paper will look over the different technologies that provide cloud services and get answers about cloud integrity between public entities.

The present study aims to contextualize the current situation of cloud computing technologies and evaluate the constraints on cloud interoperability within the European Union.

To accomplish his objective, the following milestones are defined:

- Perform the Literature Review:
    - Define Clouds types and their operability, Identify cloud owners, providers, and factors on a cloud computing environment.
    - Review of the current Cloud Computing Standards.
    - Define Survey to map potential gaps and opportunities on Public clouds.
- Identify the standards that public organizations must meet together with their legislation (EU legislation) and the benefits that these entities can achieve by using cloud services.
- Identify the internal logic and potential gaps of the cloud while it is interoperated by an organization that provides public services.
- Analysis of Survey results to draw up cloud computing map paradigm.
- Propose a solid cloud computing model for public entities.
- Validate the model describing its advantages and disadvantages.
- Envision future work.

1.3. STUDY IMPORTANCE AND RELEVANCE

Nowadays, the Internet paradigm has become the main source of data accessibility, this makes it a powerful tool for the whole kind of organization. Cloud Computing is part of an internet environment. Its potential relies on the capacity of storage and information portability linked to technological advances within organizations.

This research aims to explain and establish/propose the foundations of what a structured public cloud model can be and explore the opportunities that Cloud Computing can offer from the user's point of view.

The relevance of interoperability between clouds is the free fluctuation of information between public entities like it can be the European Union where administrations portability has not been deployed yet (Chastanet, Shaping Europe's digital future, 2019). This document will lay the foundations for modeling a standardized cloud computing model that allows EU citizens and organizations unique benefits and advantages like ubiquity, convenient on-demand network access aligned with a European strategy.

These advances in the public administration field will promote the wide take-up of cloud services by enhancing trust and confidence, notably through interoperability, data-portability, data protection, and security (Chastanet, Shaping Europe's digital future, 2019).

2. LITERATURE REVIEW

2.1. CLOUD COMPUTING

The hype surrounding cloud computing has been noticeable during the last decades. We can find lots of definitions about what's cloud-computing and how this new tool has deployed new capabilities and value to companies, users, and providers.

This chapter will review and define the components of cloud computing. Moreover, we will take an overlook into the different kinds of clouds that can be hosted by public or private providers, in other words, the interoperability and cloud domain can be managed by organizations that will have unlike levels of constraints depending on the character of the entity.

To define what cloud-computing is we can stick and get an accurate and accepted definition from the National Institute of Standards and Technology (NIST) previously defined in 2009 and ratified in 2011 by the industry:

> *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"* (NIST, 2011).

The cloud is composed of multiple servers linked within a network that will allow the communication within servers using communication protocols, nowadays this communication is through open specifications language. e.g. Web Services. (Gorelik, 2013).

2.2. TYPES OF CLOUD COMPUTING

There are three commonly used cloud deployment models: private, public, and hybrid. An additional model is the community cloud, which is less commonly used.

A private cloud is built and managed within a single organization. Organizations use software that enables cloud functionality, such as VMWare, Cloud Director, or OpenStack. (Gorelik, 2013)

A public cloud is a set of computing resources provided by third-party organizations. The most popular public clouds include Amazon Web Services, Google AppEngine, and Microsoft Azure.

A hybrid cloud is a mix of computing resources provided by both private and public clouds. A community cloud shares computing resources across several organizations and can be managed by either organizational IT resources or third-party providers.

2.3. COULD COMPUTING CONCEPTS

2.3.1. Cloud consumer

A cloud consumer is a principal stakeholder for the cloud computing service. A cloud consumer represents a person or organization that maintains a business relationship with and uses the service from a cloud provider. A cloud consumer browses the service catalog from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service (NIST, 2011).

The cloud consumer may be billed for the service provisioned and needs to arrange payments accordingly. Cloud consumers need SLAs to specify the technical performance requirements fulfilled by a cloud provider. SLAs can cover terms regarding the quality of service, security, remedies for performance failures.

A cloud provider may also list in the SLAs a set of promises explicitly not made to consumers, i.e., limitations, and obligations that cloud consumers must accept (Marek Moravik, 2018). A cloud consumer can freely choose a cloud provider with better pricing and more favorable terms.

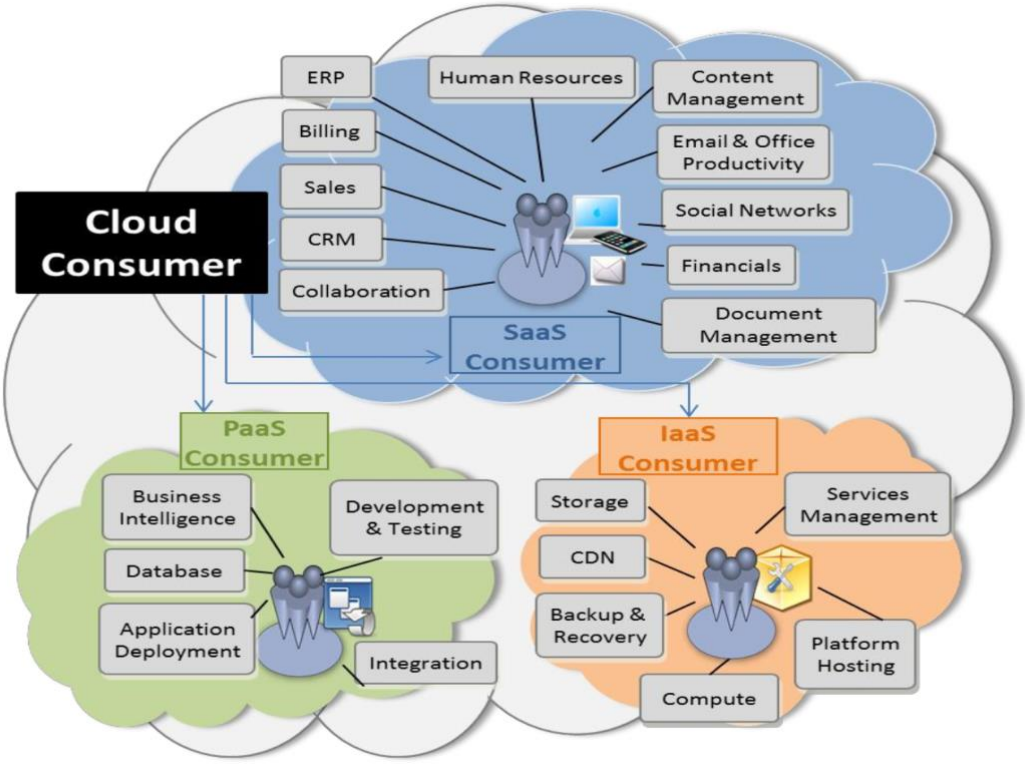

Figure 1. Cloud Consumer services (NIST, 2011).

2.3.2. Cloud Provider

Other than defining the concept of cloud computing, we have other components to consider. Cloud providers are entities that provide the servers, virtual hardware, and most of the time the software that's used to interact with the cloud (NIST, 2011).

As mentioned before in this paper, there are different types of clouds defined by the type of organization that hosts the cloud servers.

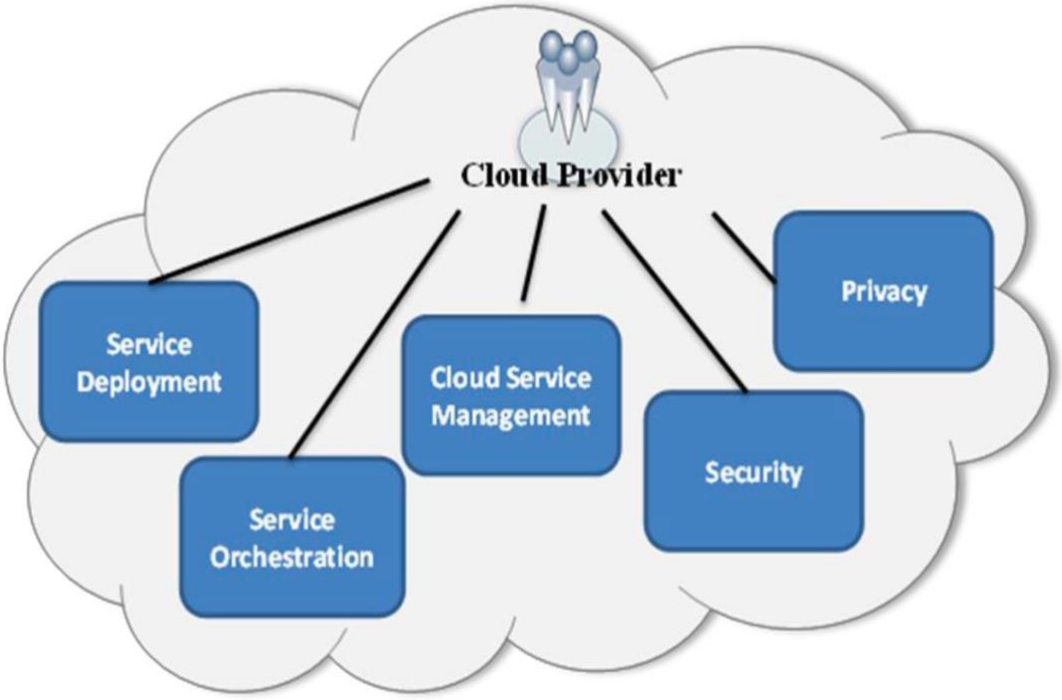

Figure 2. Cloud provider major activities (NIST, 2011).

2.3.3. ISO/IEC Main cloud computing standards

The rise of Cloud Computing technologies catalyzed the need to offer standards to regulate and establish the bases of a reference model of Cloud. The organization in charge of publishing the norms are ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). Both hardly work on setting and architecture and the reference model for Cloud Computing by analyzing and compiling all needs to categorize various scenarios, from basic standards up to deep Cloud computing environment such as security terminology.

In this section, we will mention and review the standards purposed by the organizations in charge of publishing such standards. These standards will spare into two different areas: a reference model a regulation framework to secure data within a cloud computing environment.

2.3.3.1. ISO/IEC Cloud computing Standards bases for a conceptual and architecture

Terminology definition of Cloud computing resources:

To unify the comprehension of Cloud Computing and provide a base for acknowledging CC terminology standard terms are grouped into the next ISO/IEC norm.

- **ISO/IEC 17788 (2014):** To set the base for acknowledging the terms of CC they are set into a group of standards related to the environment of the cloud in the 17788 standards series. They are specific and linked to data management including confidentiality, integrity, interoperability, data recovery, and availability.

An architecture reference model for Cloud Computing:

- **ISO/IEC 17789 (2014):** Specifies the reference architecture model in terms of technical requirements from a user and function perspective. In this reference model the role, tasks, functional components, and relation between such elements within the Cloud Computing environment are set into 17789 series.

Cloud computing services environment definition and data usage:

To classify data from cloud services and to specify the use of data in Cloud Computing environments, the ISO / IEC 19944: 2017 standard established that:

- I**SO / IEC 19944 (2017):** Extends existing Cloud Computing terminology and reference architecture in ISO / IEC 17788: 2014 and ISO / IEC 17789: 2014 to describe an ecosystem involving devices using services on the cloud; describes various types of data that flow within devices and the cloud ecosystem; Fundamental concepts are provided, including a data taxonomy; The categories of data flowing through customer devices and cloud services are also identified. It can be used for transparency on how data is used in an ecosystem of cloud devices and services.

Enhancers and enablers of cloud computing good practices for standardization between Cloud consumers and providers:

To improve and standardize service agreements between suppliers and customers, the ISO / IEC 19086-1 / 4 series is developed. Together, this series provides an overview of cloud service level agreements, clarifies the relationship between cloud service agreements (CSA) and cloud SLA, and offers customers and cloud service providers a common understanding of the concepts, terminology, metrics, and requirements necessary to establish a cloud SLA. The main idea of each part of the ISO / IEC 19086-1 / 4 series is as follows:

- **ISO / IEC 19086-1 (2016):** An introductory model is established that can be used to create SLAs in the cloud, providing: an overview of SLAs in the cloud; identifying the relationship between a CSA and a cloud SLA; the concepts that can be adapted to create an SLA in the cloud; and the terms commonly used in cloud SLAs. This standard is intended to make it easier for clients when comparing services from different cloud service providers and to allow them to identify the most important points to value in their cloud projects.
- **ISO / IEC 19086-2 (2018):** A technical model is defined to document the metrics of SLAs in the cloud and applications of the model are included with examples. This standard establishes a common approach and terminology for specifying metrics.
- **ISO / IEC 19086-3 (2017):** The main requirements and guidance on target compliance for cloud SLAs are regulated.

- **ISO / IEC 19086-4 (2019):** Requirements and guidance for security and protection of personally identifiable information components for cloud SLAs are specified.

Interoperability incentive standards:

To promote interoperability and portability of cloud computing, the ISO / IEC 19941: 2017 standard is developed.

- **ISO / IEC 19941 (2017):** The types of interoperability and portability of Cloud Computing, the relationship, and interactions between these two transversal aspects are specified; also, the common terminology and concepts used to discuss interoperability and portability, particularly to cloud services. The goal of this standard is to ensure that all parties involved in cloud computing have a common understanding of interoperability and portability for their specific needs. This agile an understanding of interoperability and portability in Cloud Computing environments by establishing common terminology and concepts.

In conclusion, the standards above are primarily taken from the perspective of user groups of cloud computing stakeholders, including cloud customers, providers, developers, and auditors, formulating standards according to various requirements and needs of these users. For enterprise and postgraduate type users, it is necessary to master the expressed standards, use cloud services reasonably and normatively, and achieve optimal information management in the Cloud Computing environment.

2.3.3.2. Cloud data protection and regulation standards

Requirements for Cloud computing security and guidelines:

To review the standards formulated by ISO and IEC for the regulatory framework of information security and data protection in the Cloud Computing environment from the following approaches.

The first approach focuses on the guidelines, requirements, and management of information security in the cloud; Likewise, the applicable regulations are detailed below:

- **ISO / IEC 27036-1 (2014):** This is an introductory part of the ISO / IEC 27036 series, which is a four-part guide series on security in supplier relationships. An overview of the guideline is provided to help organizations ensure their information and information systems security within the context of supplier relationships.
- **ISO / IEC 27036-2 (2014):** The fundamental information security requirements are specified to define, implement, operate, monitor, review, maintain and improve relationships between suppliers and buyers.
- **ISO / IEC 27036-3 (2013):** Products and services in the ICT supply chain are provided to buyers and suppliers with guidelines on information security risks.
- **ISO / IEC 27031 (2011):** All security-related events and incidents that may have an impact on ICT systems and infrastructure are covered. It includes and extends to information security incident management practices and planning and preparedness management for ICT and services.

Management and risks security assessments into cloud computing services:

The management risks and information security controls in the cloud are listed below:

- **ISO / IEC 27036-4 (2016):** Provides cloud service customers and cloud service providers with guidance on the one hand, gaining visibility into the information security risks associated with the use of cloud services and managing them effectively; on the other hand, respond to specific risks of acquisition or provision of cloud services that may have an information security impact on the organizations that use these services.
- **ISO / IEC 27002 (2013):** This is the code of practice for information security controls. Guidance is provided for the organization's information security standards and information security management practices, including the selection, implementation, and management of controls, considering the information security risk environment of the organization. organization.
- **ISO / IEC 27017 (2015):** Provides guidelines for information security controls applicable to the provision and use of cloud services, offering: additional implementation guidance for the relevant controls specified in the ISO / IEC standard 27002: 2013; and additional controls with an implementation guide that specifically relate to cloud services.

These standards provide controls and implementation guidance for both cloud service providers and cloud service customers.

ISO/IEC focused on personal data protection and privacy into a cloud environment:

Regarding the protection of personal data and privacy in the cloud environment; Likewise, the relevant standards are presented below:

- **ISO / IEC 29100 (2011):** Provides a privacy framework that specifies common privacy terminology; that defines the actors and their roles in the processing of personally identifiable information (hereinafter PII); describing privacy protection considerations; and that it provides references to known privacy principles applicable to information technology, including Cloud Computing technology.
- **ISO / IEC 27018 (2019):** Generally accepted control objectives, controls, and guidelines for the implementation of PII measures are established by the privacy principles of the public cloud computing environment in the ISO / IEC 29100 standard 2011, considering the regulatory requirements for PII protection that may be applicable in the context of the information security risk environments of a public cloud service provider. In addition, the ISO / IEC 27018 standard allows cloud service providers whose infrastructure is certified with this standard, to tell their current and potential customers that their data is guaranteed and that it will not be used for any purpose for which it does not your consent is expressly given.

In conclusion, the above-mentioned international standards, from the perspective of the cloud service provider and customer, the information security monitoring system in the cloud environment is tackled, which is beneficial to provide a source standard for international cloud security certification. Regarding the cloud industry security

certification and compliance with it, it is a pre-requirement for the formal operation of any cloud service provider, and it is also a guarantee to provide the customer with cloud services.

Finally, at the international level, we can tell that all these standards around cloud computing are more complementary and form a relatively complete system. It is allowed to guarantee the rights of users and service providers in the standard aspect and favor business users and individuals to choose high-quality operators that can protect the security and privacy of their data.

2.3.4. Cloud Security

One of the main key factors on Cloud Computing and Audits in these environments is evaluating and recognizing security gaps and potential impacts on data transfer cloud to cloud. Security is a cross-cutting aspect of the structure affecting all layers involved in a cloud computing reference model (Ahmed Taha, 2017).

Therefore, security does not rely solely on cloud providers but also on consumers and other factors/actors.

Standard security measures on cloud-based systems can be addressed requiring such parameters as authorization, authentication, integrity, audit, network availability, confidentiality, identity management, security monitoring, incidents response, and security management. Most of these security factors are already implemented, and they are not new, but no they are relevant to analyze, discuss and implement security parameters in a cloud system (Ahmed Taha, 2017).

2.3.5. Security Based on Model Perspectives

Having in mind the different existing cloud services; SaaS PaaS and IaaS, consumers must have distinct management services operations that will expose entry points into cloud systems that can be attacked or threatened by adversaries or competitors (NIST, 2011). Hence, security must be considered based on the Cloud service type model to consider the impact and how to address different threats.

2.3.6. Shared Security Responsibilities

The level of implication and relevance on security implication of the Cloud differs depending on the exclusivity and deployed cloud. Private clouds are dedicated only to one consumer or organization, public clouds have unknown tenants co-existing in the same cloud environment.

Cloud providers and consumers need to collaboratively deploy, operate, build, and design the cloud-based system. Dividing the control between these two actors means sharing responsibilities in providing certain security standards for the cloud (Fang Liu, 2011).

It can be determinate the level of responsibility by the cloud service models implying different degrees of security control between Cloud consumers and providers.

2.3.7. Privacy

Cloud providers should protect the assured, proper, and consistent collection, processing, communication, use, and disposition of personal information (PI) and personally identifiable information (PII) in the cloud.

According to the Federal CIO Council, one of the Federal government's key business imperatives is to ensure the privacy of the collected personally identifiable information. PII is the information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. (Fang Liu, 2011) Therefore, Cloud Computing (CC) combines shared resources and responsibilities as a flexible solution for data but, at the same time, it is clear that additional challenges have to be taken into account by consumers and providers while using Cloud Services.

2.3.8. Service Level Agreements

An SLA is a contract that describes the level of services offered by a cloud provider. In the case of cloud services, SLA could be measured in terms of the mean time between failures, mean time to repair the outage, and other operational metrics such as network response time and system performance. (Gorelik, 2013)

As per diligence companies must carefully review a cloud provider's SLA agreement. Not every cloud provider can offer the level of business continuity required by organizations. Even cloud providers as large as Amazon provide only 99.95% guaranteed annual uptime for their servers, while some organizations require 99.99% annual uptime (Ahmed Taha, 2017). If service uptime drops below 99.95%, per Amazon's agreement customers are eligible for a service credit equal to 10% of their bill. Consider that Amazon's SLA does not constrain the length of downtime - unless your servers are collapse for two hours or 10 days, your company still receives the same compensation amount.

Interdepartmental services between IT and other departments inside a company are typically 331 defined by operational level agreements (OLA > An OLA describes support responsibilities between each of these internal groups). (Scott Dowell, 2014)

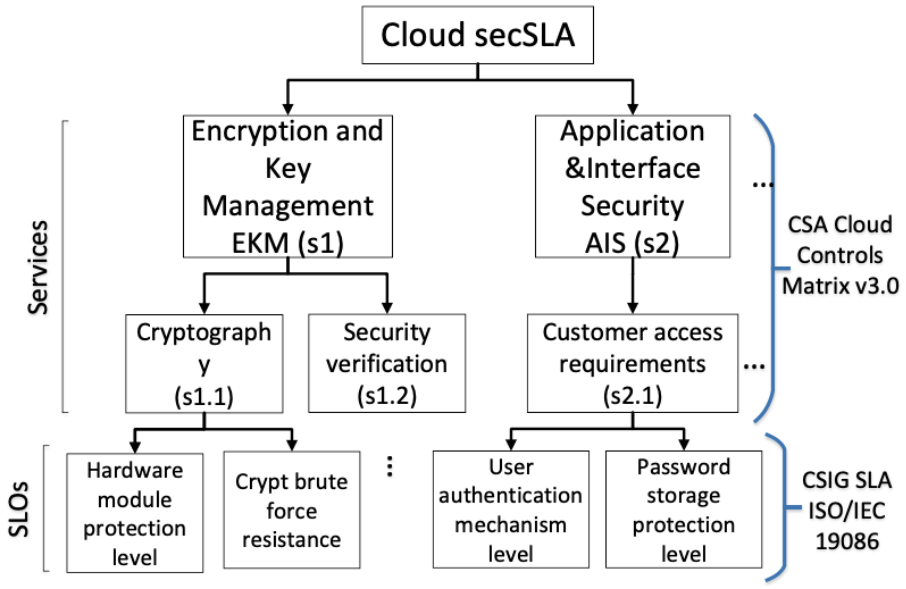

Figure 3. Cloud Security SLA Hierarchy (Scott Dowell, 2014)

2.3.9. Contract Process and risks assessments for consolidating Cloud Computing for Data Portability/Integration

The procurement of cloud providers and architecture model must be determined by the contractor, in this case, the governance and deployment for a cloud computing service must follow the requirements established by the country's legislation and government.

Technically, the difficulty of compatibility and integration of data in data centers located in a public off-premises cloud con face different challenges and risks that need to be assessed before contracting off/on-premises Cloud computing infrastructures.

Organizations that consider using a hybrid cloud where data is spread across both private and public clouds may face data integration problems:

- Security issues (data governance, network connectivity, etc.)
- Problems with transaction integrity (inability to support transactions across clouds).

That is why the process of contracting Cloud Computing services for public administration, differs between EU countries. Defining the levels of capabilities, availability, and service known as SLA levels, have to be periodically reviewable following a designed framework defined by authorities of each country.

The complexity of the process to fully integrate Cloud Services might be constrained by the legislative situation of the country. In most cases, the cloud computing policies should be accompanied by laws according to digital politics.

Also, the cycle of the contract has to be defined by between authorities and Cloud providers according to IT advances to deploy and develop new IT solutions capable of migrating the data between contracts and IT cycles.

As a result, the contracted services have to stick to the adopted framework provided by the public administration following the guidelines and technique requirements. These concepts must be harmonized with country-level laws, financial statements, general data protection regulation, and further European commission agreements.

2.3.10. Software Compatibility

Cloud providers typically support a specific set of software vendors and versions. A public cloud is a shared environment, where software is shared among hundreds or thousands of isolated customer environments (Schnappinger-Gerull, 2015). The cloud provider must maintain well-defined software standards, and therefore in many cases, cloud providers cannot offer custom software packages installed to customer clouds. Particularly for PaaS or SaaS clouds, the level of control over software is extremely limited. Companies must ensure that software in a public cloud is compatible with what they use internally.

2.3.11. Cloud Computing standards for Interoperability

As Cloud computing technologies advance, the footprint of interoperability, technology matureness becomes more relevant. These features will play key aspects on system-to-system engineering about the framework and compatibility between clouds (Scott Dowell, 2014).

To determine the amount of data system interoperability, the C4ISR Architecture Working group, published the Levels of Information System Interoperability (LISI) that classifies the complexity between systems and services towards systems in terms of Procedures, Applications, Infrastructure, and Data (PAID) (Scott Dowell, 2014).

- **The procedures (P)** are the level of interoperability that gets from the operational policies and processes, like functional program development guidance, compliance of technical and systems architecture standards.
- **The Application (A)** results from the power of the software package to work with and on other systems.
- **The infrastructure (I)** attribute reflects how the systems are connected between them using different applications such as point to point of wide-area network communications involving different protocols and the way they interact between them.
- **The Data (D)** represents the format of the data and therefore the flexibility of it to be exchanged between system domains.

Apart from various actors in a cloud-to-cloud (C2C) network, it must be considered the maturity of the systems which have to interoperate between them. We can find five different levels of maturity:

- No interoperability or isolation system with any integration of data from different environments must be done manually. (**Level 0**).

- A Peer-to-Peer interoperability connection environment is characterized by electronic connections, spare data, and applications (**Level 1).**
- Functional interoperability in distributed environments characterized by spared data and apps in a distributed environment with basic collaborations and heterogeneous product exchange. **(Level 2).**
- Domain-based interoperability in an integrated environment characterized by wide-area networks shared data, separate applications, shared databases, and sophisticated collaboration. **(Level 3).**
- Enterprise-based interoperability in a universal environment is characterized by wide-area networks, shared data, shared applications, cross-domain information sharing, and advanced collaborations. **(Level 4).**

As a model, LISI is part of a point of view on system-to-system information exchange without deeply analyzing and providing the bases to assess the maturity of C2C interoperability, in specific, mobility and security. This is especially relevant when assessing usability and acceptability-for-use perspective.

2.4. GAIA – X PROJECT - EUROPEAN ASSOCIATION FOR DATA

The end call of EU data integration can be represented in what's called GAIA – X Project.

This project initiative pretends to be the enabler and main guideline that aims to consolidate an EU Cloud Computing system that will provide services across frontiers within the EU. The project is a conglomerate of private and EU entities that integrates an IT cluster to develop the structure, framework, and policies to meet digital and next-generation technologies based on cloud computing services, besides other new technologies. (European Commission, Shaping Europe's digital future, 2020)

Germany and France started GAIA's X project by setting up hub data centers at the country level to incentivize local governments and other countries to embrace this project and encourage other communities to join the European Cloud Federation roadmap.

Furthermore, other private and public sectors have seen this project as an opportunity for economic growth. Italy, Spain, Portugal, Netherlands, Belgium, and many other EU members have confirmed their participation in GAIA's X publishing their Cloud Computing strategies ((BMWi), 2020).

It is seen as a unique opportunity to strengthen the European Digital Single Market and its competitiveness.

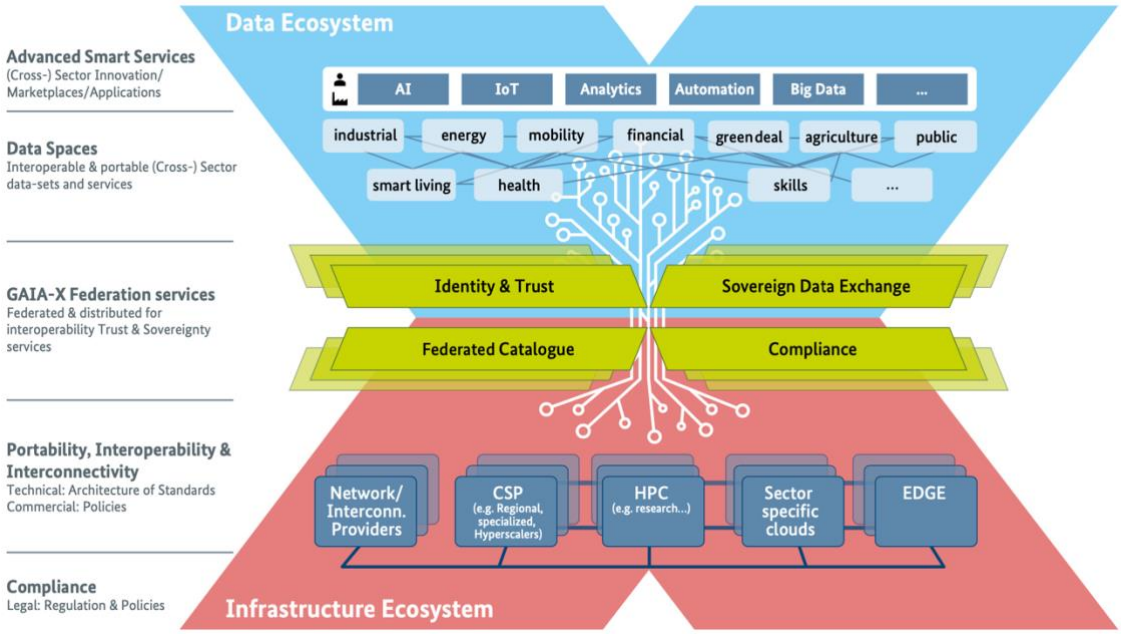

Figure 4. An architectural concept with GAIA-X federated Services ((BMWi), 2020).

The goal of the project focuses on leaving behind and working on the main deficiencies such as lack of transparency, overprocessed data, absence of an API's able to connect widely data from different EU countries and sectors. (The European Commission, 2013) Taking into account the factors mentioned before these could be considered as constraints to innovate and deploy a framework.

Furthermore, GAIA-X aims to:

- Converge Digital Infrastructures to incentivize innovation and enhance interconnected data applications.
- Increase Transparency and Trust on Digital Services.
- Reduce dependencies.

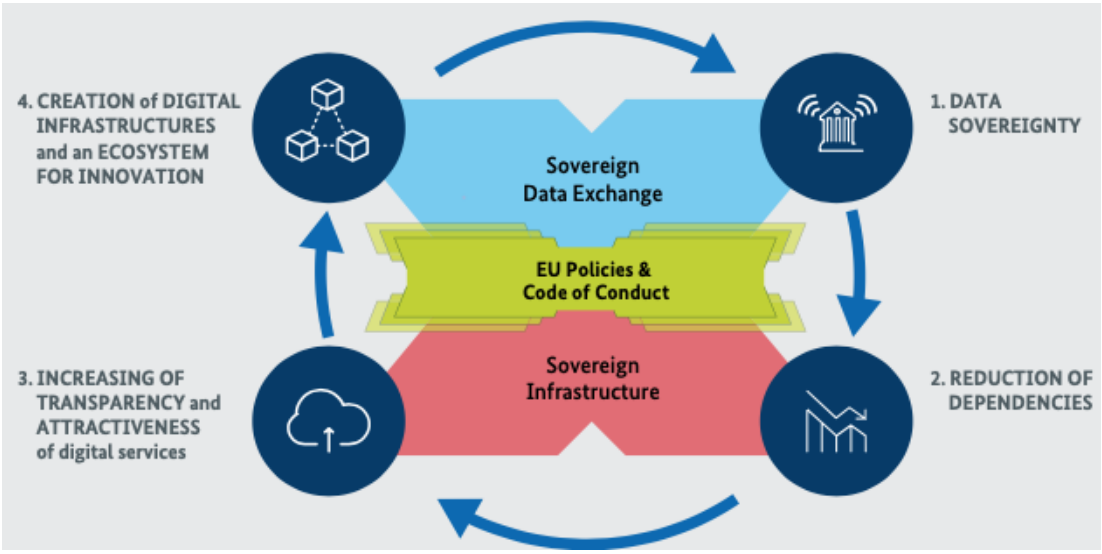

Figure 5. GAIA-X Goals ((BMWi), 2020)

GAIA-X is working to deploy and create the guidelines for orchestrating the policies, and target architecture aligned with EU commission guidance on free-flow of data and to develop an architecture of standards to uniform and ensure the interoperability between services.

2.4.1. Portugal Cloud Computing Strategy & Vision

The European Union policy regarding Cloud Computing within the former states has been projected to catalyze and increase the use of CC.

Portuguese strategy relies upon three different key factors:

1. Safety and equitable contract terms and conditions: embrace the best practices and contractual model to benefit consumers to increase engagement between the administration and their CC users.
2. Identify and standardize the CC Services: define which is the path to follow to agile and integrate administration systems to guarantee interoperability, portability, and data recovery.
3. Establish a European Cloud Partnership (ECP): Develop and deploy common requirements either for private or public sectors to approach and assess institutional transparency, digital transformation, sustainability to innovate and increase service efficiency. (CTIC, 2020)

Nowadays, some EU countries have formalized some guidelines and strategies to move their services into the Cloud, UK, Ireland, Norway, and Italy. On the other hand, some others are trying to define their strategy such as Spain, Germany, Sweden, Denmark, France.

The main strategy is defined by the same values and principles:

- Cloud solutions replace old and obsolete administration technologies.
- Develop a CC framework to work with concrete criteria analyzing risks for users.
- Prioritize CC after developing a framework that assures the best cost-benefit without any infrastructure constrain to adopt Cloud Computing solutions.

As it has been published by the European Commission, the Digital Cloud strategy has to be an enabler of Cloud Computing Services by prioritizing services in the cloud guaranteeing a secure hybrid multi-cloud service (European Commission, Shaping Europe's digital future, 2020).

The vision of Portuguese authorities relies on the prioritization of Cloud Computing Services, if possible, over other obsolete technologies (CTIC, 2020). Adopting the cloud to the administration guideline implies:

- Data protection and sovereignty of the data are critical requirements to access Cloud Computing projects.
- Public CC services solutions have priority for public cloud aligned with a defined framework for implementation.
- To minimize economic and environmental impact, cloud providers should be prioritized according to market CC available solutions.

- Public administration must closely monitor the use and quality of the service offered by the cloud computing provider.

The Portuguese government has recently joined project GAIA-X including IP Telecom company as one of the founder company's forming part of the IT & TIC cluster. Participating in this project will represent a step ahead for Portugal towards the EU digital strategy into an Atlantic tech hub (Nunes, 2020).

2.4.2. Spain Cloud Computing Strategy & Vision

The implementation in Spain has been defined into a 5-year plan where services will be updated into a digital tool such as cloud computing. These years the process has been accelerated due to the pandemic situation that worldwide affected all the administrations (Ministerio de Asuntos Econòmicos y Transformación Digital, 2020).

Transform the administration and adapting the systems to the pandemic has exposed immediate challenges that have to be approached in the next short-medium term. Spain is one of the European countries that integrates an active developing network for Europe's supercomputing program. As an example, the EuroHPC JU has agreed to be hosted by an IT cluster to deploy supercomputing features represented at Barcelona Supercomputing Center (BSC).

Therefore, the adoption of Cloud Computing services is key to transforming and updating the administration infrastructure. The strategy proposed by Spanish authorities combines private and public clouds to reduce synergies and environmental impact by enhancing AGE services (Administración General del Estado) towards the private sector and delivering public services for specific needs.

This way the public administration, can explore different IT providers to offer the best services in 360 degrees managed by the central administration.

(Prof. Alan R. Hevner, Design Science in Information systems Research, 2004)

There are two topics that Spanish authorities will focus on to deploy CC services:

1. **Prioritize Cloud Computing services based on Cloud technology.**

   These resources will be complemented with cloud computing solutions provided by the private sector. Privacy and data protection will be fundamental to access any public contract.

   The main goal of prioritizing CC services is to consolidate Governmental Administration Data Process Centers to reduce economic and environmental impact.

   Also, the consolidation of these centers will improve the participation of Spain in initiatives such as the EU Cloud Federation and GAIA-X Projects.

2. **Reinforce of Cloud services intragovernmental into EU context.**

   The participation of the different administrations in the cloud computing interrelated services will be key for deploying an EU cloud computing service environment. Spanish Administration will follow the Cloud Federation directives and

NIS directives to achieve compatibilities and requirements that benefit their projects regarding cybersecurity and public networks within the EU.

As per the initiative, the Spanish strategy passes by taking measures to create new state structures to monitor the governance of the data. The Spanish government will create the Chief Data Officer (CDO) to guarantee data usage behavior and orchestrate the guideline to allow private and citizens access to public administration data (Ministerio de Asuntos Econòmicos y Transformación Digital, 2020).

3. METHODOLOGY

3.1. DESIGN SCIENCE RESEARCH

To develop a framework to support a model that is compatible by implementing a Cloud Computing model a solid methodology will determine if the goal is achievable.

The methodology will be supported by a designed cycle scheme proposed by Alan R. Hevner. This model is a significant opportunity to contribute to the research by considering a design-science and behavioral-science approach to solve and conduct Information Systems (IS) applications research. (Prof. Alan R. Hevner, Design Science in Information systems Research, 2004)

This model aims to address, evaluate, and present design science research. To tackle the different actors and behavior of the model, there's the need to describe the boundaries between the IS and the science design. To do so, Hevner proposes several guidelines for conducting design-science research.

Information Systems and Cloud computing and the organizations they support, tend to be complex and meticulously designed. To illustrate the relevance between business and information technologies strategy, Henderson and Venkatraman (1993) propose an alignment model create an effective IS infrastructure.

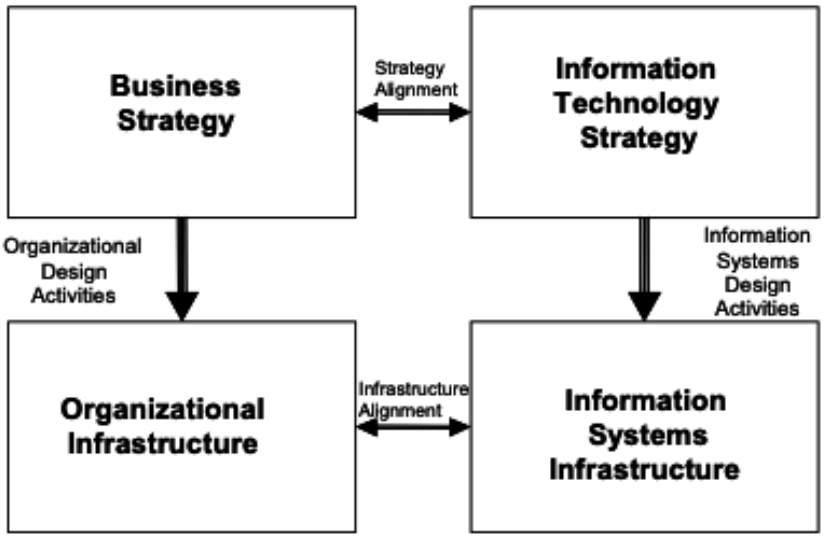

Figure 6. Organizational Design and Information Systems Design Activities (Adapted from J. Henderson and N. Venkatraman, Strategic Alignment: "Leveraging Information Technology for Transforming Organizations," IBM Systems Journal (32:1), 1993.)

The paradigm proposed by Henderson and Venkatraman (1993) must face an important dichotomy. The design represents the process and a product. This perspective turns continuously between design processes and artifacts for the same problem to retroactively enhance themselves. (Prof. Alan R. Hevner, Design Science in Information

systems Research, 2004) To be more specific, a design process is a sequence of activities that have as an output. A product (artifact).

The goal of this paper is to design a science research framework to validate and confront Cloud Computing services hosted by different providers and consumers compatible between them.

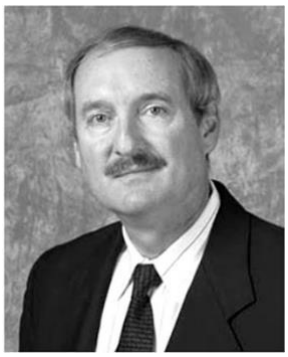

Figure 7. Prof. Alan R. Hevner, Ph.D. RERO Doc digital library archive.

To better understand the complexity of the problem Alan. R. Hevner proposes a conceptual model divided into two main areas: Environment and Knowledge base. These two converge into what's called IS Research to validate and justify the artifact as part of the solution.

Environment: describes the space where reside the problem is to solve. In this area, the business needs identified are set into goals, opportunities, tasks, and problems perceived by the organization's people.

IS Research DSR: considers the people, organization, and available technologies. Each of them has defined goals, activities, and opportunities that define the need to research. (Prof. Alan R. Hevner, Design Science in Information systems Research, 2004). This area will shape and validate a purposed and viable strategy to solve the problem faced.

IS research area involves two different subcategories that are conducted through development and justification phases. Both are complementary and aim to design a model based on behavioral knowledge to confront the root of the business need and utility of the purposed solution.

Knowledge base: It is the area that feeds the DSR research model of the different behavioral theories, information, models, models, etc. providing applicable knowledge to the research study. (Prof. Alan R. Hevner, Design Science in Information systems Research, 2004)

To represent the model to justify the resources and outcome of this paper the methodology framework to follow is defined in *Figure.7.*

(Prof. Alan R. Hevner, Design Science, 2018) (Prof. Alan R. Hevner, Design Science, 2018)

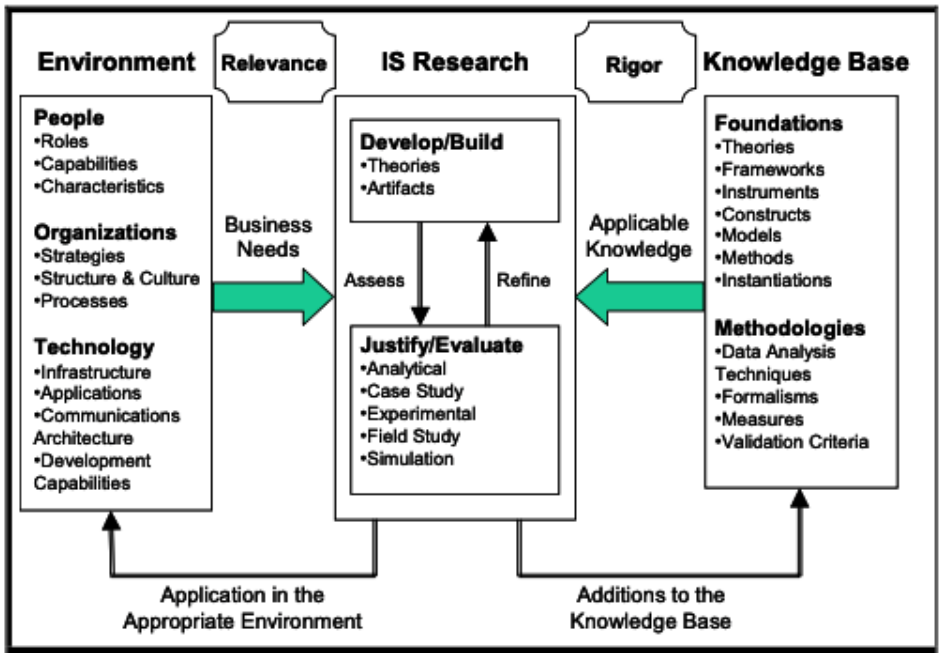

Figure 8. Hevner et al./Design Science in IS Research. Information System Research Framework. (Prof. Alan R. Hevner, Design Science in Information systems Research, 2004)

As explained before, DSR is designed to formulate a problem-solving (Prof. Alan R. Hevner, 2018) process. The basis for deploying these solution research processes are seven guidelines inferred into knowledge and understanding of a process issue and its arrangement obtained by building an application of an artifact.

Guideline	Description
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Table 1. Hevner et al./Design Science Research in IS Research. Design-Science Research Guidelines. (Prof. Alan R. Hevner, Design Science in Information systems Research, 2004)

· **G1 - Artifact Design**: The final goal of DSR I is to create or enhance an artifact that addresses an issue within processes systems for organizations or business needs.

However, to approach an artifact the spectrum is narrower as we do not take into consideration actors included in a system environment, such as people and elements of an organization to define the artifact nor the evolution of it over time (Prof. Alan R. Hevner, 2018).

We conceive an artifact not independent from the environment and context within the organizations, but ad interdependent with them by meeting their needs. Furthermore, an artifact developed on a DSR is not a full-grown system by itself. Instead, they defined innovations or ideas aiming to solve the organization's needs. Specifically, provides the core symbology and vocabulary to define the problem and solution, which has a significant impact on the tasks that need to be tackled and the definition of the problem to address.

· **G2 – Problem Relevance**: The goal of a DSR in IS is to acknowledge that implementing a tech-based solution is relevant to problems not solved until to date. Developing innovative artifacts explores new phenomena to occur within business needs, consequently, the artifact enables organizations to predict and overcome future problems acceptance.

Precisely, describing and defining the relevance of a problem drives to find the differences between the current state of a problem into a new state of a system to research a potential solution. Hence, business opportunities often raise from an effective analysis of business processes problems that can be solved.

These changes mainly impact the community or organization involved in the system environment heading to address the problems faced by interacting with the Information system process.

· **G3 – Design Evaluation**: The functionality of an artifact must be rigorously evaluated by demonstrating its quality, utility, and efficiency. Hence, evaluating requires deploying and integrating the artifact into the system environment. The evaluation phase provides constant insights and feedback to build a solid model. Nevertheless, the evaluation methods are subject to the technologies available in the development phase. Therefore, assumptions might change from prior research studies since they might be deprecated.

Evaluation methodologies for designed artifacts frequently use data available at the knowledge base area. These methodologies can be based on; **observational, analytical, experimental, testing, or descriptive evaluations**.

· **G4 – Research contributions**: Effective design-science research must provide a clear contribution towards the design artifact underlying knowledge of design construction. Some of the contributions must be detected in a DSR project at the following phases i.e. The design Artifact, Foundations, or Methodologies.

To accurately contribute to the DSR system and represent the advances in the research the criteria to assess the contributions must be accurately representational and pragmatically implementable within the system environment.

· **G5 – Research Rigor**: The tutelage of a DSR must be conducted with rigor to address the problem as well as the methodologies disclosed. Rigor is usually assessed by the adherence and data collection for proper analysis techniques based on mathematical or

behavioral theories towards the DSR artifact. Rigor is the result of a well-driven knowledge base.

· **G6 – Design as a Search Process**: The nature of design a process requires an iterative search process to discover and self-assess the solution domain for the business need. For designing an effective solution there are sets of resources and actions to build the solution considering the constraints within the environment and the goal of the proposed solution.

However, one designed solution can be subdivided into another set of possible design solutions for specific problems for satisfying some constraints compliance.

· **G7 – Communication or Research**: The need to concisely communicate the DSR is relevant to approach weatherly tech-based and management-oriented. This enables the parties interested in the benefits offered by the artifact of the study to be considered for implementation within a specific organizational context. Therefore, communication mechanisms focused on the specific audiences might be applied.

3.2. RESEARCH STRATEGY

This study is based on a qualitative paradigm and exploratory nature. The description and results are an analysis of the concepts reviewed in previous chapters and ratify the purposed artifact to follow the guidelines accepted by the international community and validated by the International Organization for Standardization (ISO).

Specifically, this research will list the relevant ISO standards for public cloud services and will analyze the results from interviews of Cloud network specialists that will contribute by providing insights of the ISO standards listed to accomplish the checklist to identify potential gaps on public cloud computing services that could be addressed by ISO standards.

3.2.1 Problem Relevance:

Positioning cloud computing at the center of auditing makes this role a guarantee of the functionality, management, and identification of potential risks and opportunities for Cloud Computing technologies and can be an important tool for determining environmental challenges.

To approach Public Organizations, Cloud Computing (CC) environment and systems, system functionality identification is key for providing the best interoperability between clouds to tackle potential risks while operating between clouds, such as conflict of interests, service levels agreements (SLAs), etc.

As a result of the literature review is possible to state that a solid model of cloud computing service for public entities must have:

- Well-defined Service-Level Agreement.
- Cloud Computing Audit Frameworks.

Nowadays, cloud environments haven't been adapted so far to any specific framework to be evaluated. There are currently some protocols like COBIT, ITIL, and others that are

considered worthwhile control mechanisms as part of a start point requirements to evaluate cloud computing environment systems.

- Audit security risk-based approach in the cloud computing environment and internal auditor role by Public Orchestrator.

Understand the purpose of the technology, establish, an approach for risks and develop effective solutions for those risks.

Indeed, the main complexity of cloud computing audit is that tech carriers are usually outside the audited organization.

- Framework in Cloud computing environment.

Key Cloud Computing auditing is based on SaaS and IaaS as part of risks assessments and center of CC infrastructure.

Key decision factors in IaaS are to reduce management impact by outsourcing IaaS for efficiency-cost relation.

. Connectivity

. Network Service

. Compute Service and Management

. Data storage

. Security

Business process modeling – The need of modeling the business structure with data and applications to integrate systems between networks.

Evaluation and analysis – Considering the costs and reliability of the system integration including service levels of agreements.

Process Execution – This is the measure of controlling the different factors to evaluate the concepts mentioned above. E.g., Enterprise Integration Applications, Service Oriented orchestration.

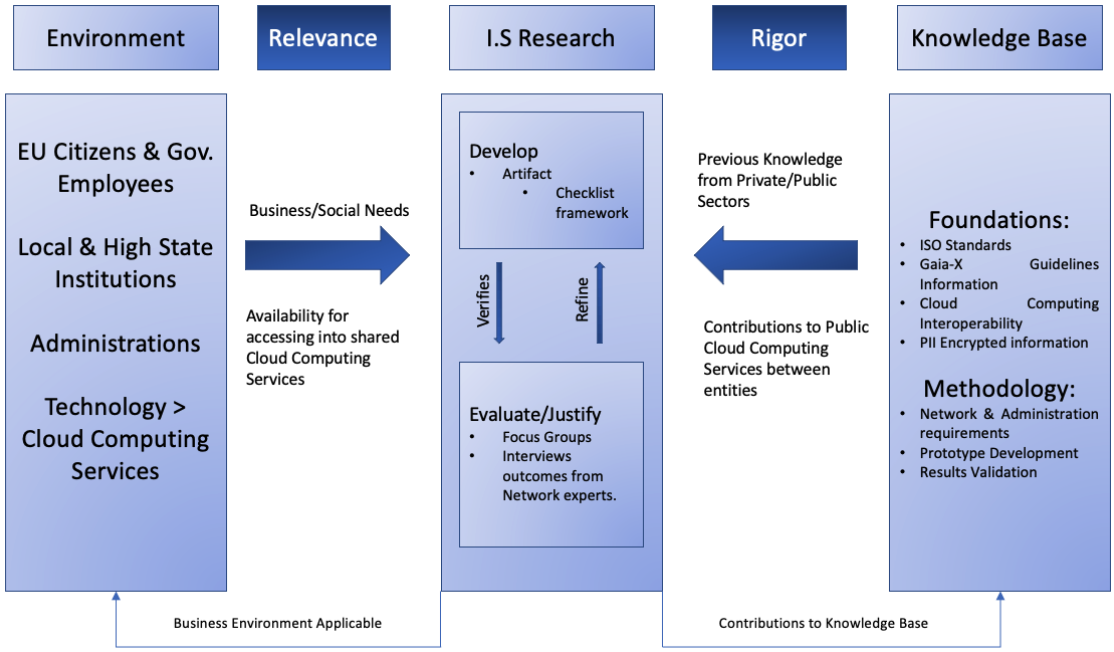

Figure 9. Information System Research Framework for Public Cloud Computing Services.

3.2.2 Research Artifact:

The core artifact to develop in this chapter refers to a Petri Network guided by the different standards that a public cloud computing service may require to share data between other organizations' clouds in the public sector.

This research artifact is based on the available technologies and ISO/IEC standards accordingly to security risks prevention **ISO/IEC 29100 (2019)** and ISO/IEC 27001 to address the best practices on data exchange performance in the CC environment.

Considering the constant evolution of the technological market, the artifact development will be constantly under review from the network and CC services users, such as citizens, experts, and administrations that will update the requirements network needs accordingly to the technologies and regulations available.

Since it has been reviewed previously, the European Union community is working on programs for developing an EU cloud computing public service.

4. REFERENCE MODEL FOR AUDITING CLOUD COMPATIBILITY.

4.1. ASSUMPTIONS

As a result of the literature review is possible to state that a solid model of cloud computing service for public entities must have:

a) SLA clearly defined

The SLA must be abounding legal format meaning to deliver services furthermore as a framework for charging for these services. Service suppliers use this foundation to optimize their use of infrastructure to satisfy signed terms of services. Service customers use the SLA to confirm the amount of quality of service they have and to take care of acceptable business models for the future provision of services. The subsequent are the main needs of the SLA:

• SLA format ought to be able to describe a service in a very clear way that the service shopper will simply perceive the operation of the services.

• State the amount of performance of service.

• outline ways in which on however the service parameters will be monitored and the format of observation reports.

• Penalties once service needs aren't met.

• State the business metrics appreciate asking and when this service can be terminated with no penalties when this service can be terminated without any penalties.

If most of the Cloud Computing Services from the EU Schengen state members have developed their clouds based on Gaia's X project these requirements are already met.

b) Trusted security model

Based on **ISO / IEC 27036-1 (2014)**, governments must protect their citizens from potential threats of the providers contracted to avoid any PII information leaks to be used against users and consumers from the administration.

Cloud encryptions must be part of encoding or re-working knowledge before it is transferred to cloud storage. Encryption uses mathematical algorithms to rework data (plaintext) that could be text, files, code, or images, to an illegible form (ciphertext) that may conceal it from unauthorized and malicious users. This is significantly relevant to confirm that cloud data can't be breached, purloined, and browsed by somebody with an unauthorized reason.

Cloud storage suppliers cipher data and pass encryption keys to the users. These keys are accustomed safely de-coded once needed to transform the hid data back to legible data.

The information that's encrypted has 3 types: *in transit, at rest, and in use.*

Data-in-transit. This kind of information is additionally referred to as “in motion”. This is often the data that's being transmitted from one place to another. It’s best to place in mind that the data transfer doesn't solely turn up between the sender and the receiver.

Data-at-rest. This data is saved somewhere while not getting used or transferred to anyone or anywhere. In this case, the Cloud Computing Servers are safely maintained.

Data-in-use. The information is intended to be in use once it's not kept in the Cloud because needs to be transferred or it is required from another Cloud. This implies that it is within the process of being erased, appended, updated, viewed, or generated.

In the following proposed model, the *in-transit* data have been already encrypted and secured to prevent any threat. The model will be focused on how this data will be transferred within a trusted and safe cloud-to-cloud environment using communications end-to-end via Simple Object Access Protocol (SOAP) requests.

4.2. PETRI NETWORK FOR CLOUD OPERABILITY

To address the CC compatibility there’s the need to write a logical system between Cloud Computing interfaces, to determine what will make the cloud eligible for exchanging information, here’s the proposal model described.

The starting premise needed is the ability to intercept all communication to and from a component, in fact isolating it from its environment. Intercepting all communication components is a requirement, otherwise, it may be impossible to adapt the behavior of components.

To context the environment of communication between clouds, there the figure (below) describes a vision of two different clouds where both are compatible as ISO standards were identified.

The initial state of the clouds will trigger an actionable request to start the flux of information requested from one cloud to another.

The model/process is composed of four main cycle steps:

a) Obsolete/Current Systems identification.

As a start point of analysis, it is required to identify the current state of the quality of the Cloud model, the ISO/IEC 1700, 1900 & 29100 will determine if the Cloud model has characteristics from two points of view, that is, system dependency and inherent standards, with some of the characteristics shared by both clouds. From the inherent point of view, data quality refers to data itself (e.g., consistency). From the system-dependent point of view, data quality depends on and is achieved by the

capabilities provided by the administration on their cloud such as the ones mentioned in 3.2.1. above. The relevance of this assessment is to comply with ISO/IEC 9941/9944 regarding systems capabilities.

b) Target Model based on Cloud Computing following ISO Standards and GAIA's X requirements.

The following model shows the Information flux between clouds from different administrations. In this case Administration A (Portugal) is requesting to Administration B (e.g., Spain) encrypted information with authorization from both sites meeting the specific requirements to send the information accordingly to ISO/IEC Standards.

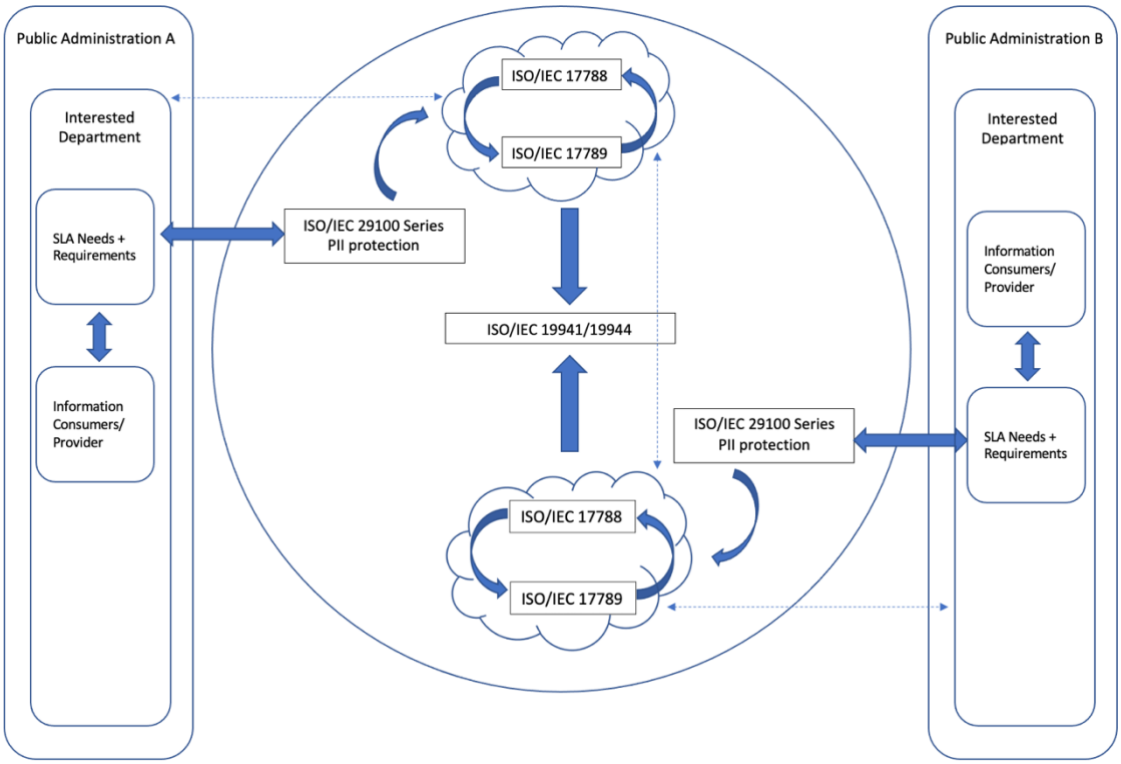

Figure 10. Cloud to Cloud environment and information Flux based on ISO/IEC standards.

c) Data PII Risks Assessment

This international standard provides a general structure for the protection of personally identifiable information, to help organizations, define the protection mechanisms related to data privacy (Jonathan Roy, 2017).

ISO/IEC 29100 It has become the privacy reference used by other ISO standards such as ISO 27001, insofar as it is required to include aspects related to the privacy of personal data.

Specifies a common privacy terminology, defines the actors and their roles in the processing of personally identifiable information. Also, provides references to privacy principles common to information technology.

The framework established in the ISO / IEC 29100: 2011 standard applies to individuals and organizations if they are using information systems or services and/or communication technologies that require privacy controls for the processing of personally identifiable information.

These standards are key for a functional cloud computing service that can interact with other administrations that will assess the compatibility and framework of the encryption and de-encryption of the data for proposed needs. The privacy framework that will safeguard PII from both clouds. Also, it provides the controls necessary to mitigate the significant risks posed to the PII (Ahmed Taha, 2017).

This standard has become a document of reference and homologation of concepts, providing clarity in the face of the plurality of national laws and regulations on the subject without coming into conflict with them and necessary to be part of GAIA's X project.

d) Implementation and Maintenance

The proposed artifact is a dynamic system $\langle N, m_0 \rangle$ is composed of a Petri net N and an initial marking $m_0 \in N \mid P \mid$, which is not more than the initial distributed state.

The evolution of the marking (state) is based on a trigger rule that responds to a logic of consumption/production of resources; It can be stated as: if there are enough resources, evolution can (it doesn't have to) take place.

A transition (*t*) is sensitized in a marked (*m*) if $m \geq Pre [P, t]$; and its shot leads to a new marking $m^1 = m + C [P, t]$. This is denoted as $m \rightarrow {}^{t} \rightarrow m^1$, and m^1 is said to be an achievable markup (from *m*). The reachability space is the set of marks achievable from m_0 and is denoted as CA (*N*, m).

Given the Petri Network $\langle P, T, Pre, Post, m_0 \rangle$, with matrix incidence C = post−Pre, if m is achievable by triggering a sequence $\sigma \in n\ T *$, that is, if m σ m, then: $m = m + C \cdot \sigma$ where σ [t] 0 - → 0 is the number of shots from *t* in *σ* (the shot counter). This equation, with variables in the natural state, is known as the fundamental equation or the equation of state.

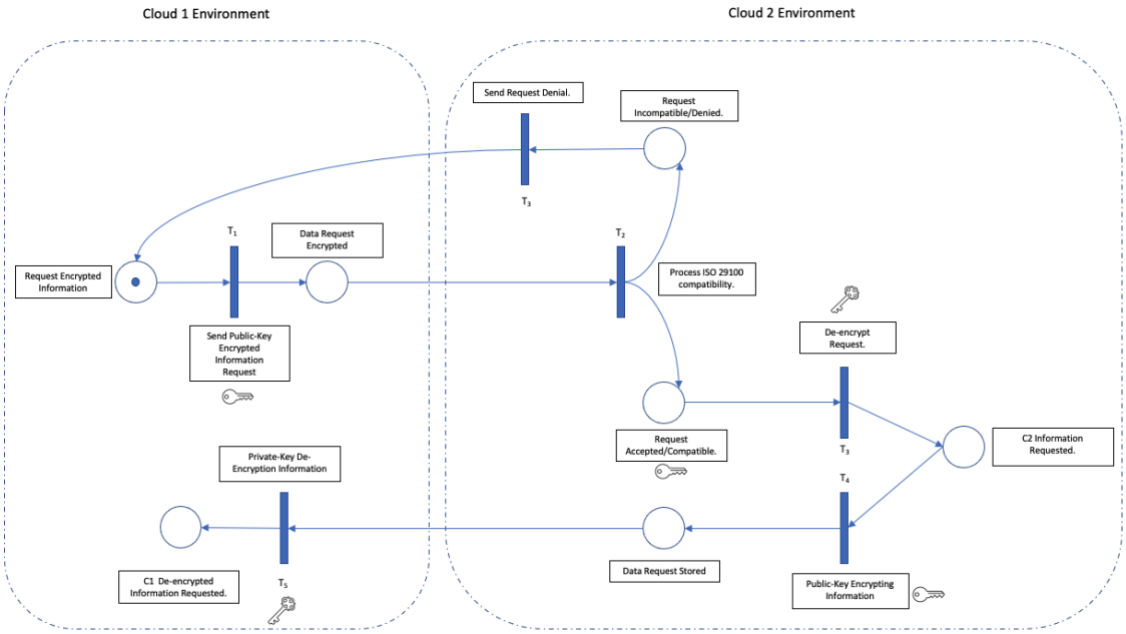

Figure 11. Discrete Petri Network for Cloud-to-Cloud data request.

As shown in *Figure 11*. the Petri network represented expresses the initial state of the system and describes each transition and state of Cloud 2 requesting information to Cloud 1.

When the requester from Cloud 1 and the receiver of that specific request from Cloud 2 share the same key to scramble and unscramble a message. It's called symmetric encryption.

Hence with symmetric encryption, the private key must be agreed on ahead of time by two organizations in private, but the Internet is open and public, so two Clouds and Organizations can't agree on private a common key.

Instead, this process uses asymmetric keys, a public key that can be exchanged with any of the public administrations, and a private key that is not shared. The public key is used to encrypt data, and any administration can use it to create an encrypted request. But the information can only be decrypted by a computer with access to the private key from the Cloud receiving the request.

Private Key	Public Key
The key is exclusively private by two administrations.	One key is publicly available while the other remains indecipherable.
Once the private key is lost the file becomes unusable.	No loss of the key since is publicly available.
It protects and encrypt data bases and sensitive information.	Commonly used to secure webs and emails.
It is a form of symmetrical encryption.	It is a form of asymmetrical encryption.
It is faster since only one key is required.	It is slower since two keys are required.

Table 2. Public and private encryption keys differences.

This way public administrations can exchange secure messages without ever needing to agree on a private key. Public key cryptography is the foundation of all secure messaging on the open Internet, including the security protocols known as SSL and TLS, which protect us when we're browsing the web.

5. VALIDATION & DISCUSSION

To evaluate and discuss the framework developed and according to the methodology followed in the paper, a deep discussion and interview with experts provided their insights from a technical point of view. The literature review was a start point to contextualize and develop a framework that confronts the experts some of the main key points for interoperating between Clouds in a public environment. The recording of the interviews was done online during 1h sessions enabled by Skype.

To validate this paper framework, specialists from Banking Clouds Solutions and CRM Cloud Solutions were selected: Joan Payeras (**JP**), Project Manager from Iberostar Group, and José Ramón Redondo Espinosa (**JR**), Cloud Solutions Analyst for Eberis Bank.

After presenting the proposed framework (Figure 10.), the interviewed experts were asked about the pros, cons, and reliability of the system to collect their insights and suggestions. (Table 2).

Q1	Do you consider the proposed framework to be useful?
Q2	What do you think are key points to consolidate the proposed framework?
Q3	Why do you think the EU GAIAs project and Cloud Computing Integrity are hard to achieve? What do you think would be the benefits of having a unique European Cloud?
Q4	Do you have any recommendations/suggestions on the proposed framework?

Regarding Q1 these are the following answers:

JR: Well, initially this looks like it would be end-to-end encryption, both in terms of the “request” and the information exchanged, so that end-to-end encryption would be done with two keys. A public key that would have both the users the one issuing the "request" and the Cloud receiver of the request, which would use the same key.

Then a private key would be generated by who is issuing the "requested" information and sends it to Cloud receiving the request. In this way, without going into much technical detail, once the user encrypts his request with the data he is requesting, he will have the private key at one end and the public key on the other Cloud.

Once the server receives it, with your private key. It would be able to unblock this encryption and get the information from the request. After the necessary validations on this request, it would return an encrypted response in the same way. The user would receive it and decrypt it in the same way that it is decrypted on the server.

I think the request and the Information should be encrypted and I'll explain why. Many times, data leaks are usually due to the request. If you send an unencrypted request, the information might reach or be intercepted by some external agent that might know the required data and issues it again, obtaining the information fraudulently in return.

On the other hand, an encrypted request intercepted by an external agent won't be able to decrypt the request as he won't have the private key that the requester Cloud uses to decrypt. So, they could not do any type of data or code injection or any other fissure or vulnerability that occurred during the service nor request.

JP: Right. I completely agree with your framework. We, for example, at Iberostar, what we do with payment information is that we do not save it. For example, credit card payment information and related information.

On the other hand, one thing that we keep since we contracted the cloud and own the web page is the user accounts and the "password".

The "password" is encrypted at the source for security if there was someone who wanted to intercept the communication. The malicious agent could not find out the password of that client and be able to see personal or sensitive information.

Regarding Q2 these are the following answers:

JR + JP: It depends on, and where we want to go. We have different options, the first one, would be if we want to save everything (data requests and information). If we want to save all the data, we receive. In that case, the safest thing and what will surely follow the regulations is going to be to make complete encryption of the entire Cloud and its information. The pro is that it becomes very secure information. The cons are optimization.

It would slow down the data flow a bit, although it would not have a big impact either, it will slow down the data requests. Having encrypted the information, send it, and decrypt it, respond to the request, re-encrypt it, and decrypt it again. This would be the way if we want to keep the information.

The second option or way would be yes, the information will only be necessary during the request and only keep it alive during the request and then the information is not stored anywhere. It is eliminated, it disappears, it is lost, or becomes nothing.

On this second type, we can have, for example, a name base, a database where we have all the names and IDs of people.

Imagine receiving a request for information that we need to know from one Cloud to another. The DNI of X person, in this case, would not need to save the data of the person, we would make the existing data visible only while the request is being made. Afterward, it would not be necessary to do complete encryption, since once the request dies and the response to the request is already done, both the information (data) and the request cease to exist. Then there is no possibility and no probability in which a data leak can occur.

The most common risk is always human error. That is, no matter how much security you put, if the human fails, the system can be as well done as you want, it will fail.

Another very common error, which usually occurs during data uploads during massive data runs, whether in the cloud or on a server itself. Bad practices, lack of security or protocols, can cause that data that we migrate to end up staying on the device of whoever does the upload locally or that they forget to upload the files and

end up in the hands of those who should not, and so on. These are usually the most common mistakes and faults that are often seen on a day-to-day basis.

In your framework and any communication between clouds vulnerabilities must be addressed, the ones generated by software itself, because of its development, its structure, its architecture…and through the hardware, whether there are external devices, such as USBs, a printer, fax, a landline. Any device that is on what would be the network or directly connected to any device that is within the network is a hardware vulnerability being infected by malware.

Regarding software, can be because it has a structure that does not follow a restricted flow where requests have an origin and an end, so there is no option to stay in an infinite loop sending a response to infinity and beyond or at the architectural level, because it is not well defined, that must remain encrypted, that it is useful to save and what is not, etc.

Therefore, I understand that there is a part of the responsibility of the Cloud provider and another part of the responsibility of the consumer as a client.

As a suggestion, we would recommend working with SOAP requests between clouds. Unlike REST requests, SOAP requests force you to identify yourself.

Meaning that before you can proceed with data recovery or request, you must identify yourself, and be given an identifier. When you pass me the identifier, then I can ask for the information. It is a way of knowing who you are before passing the data to you.

Regarding Q3 these are the following answers:

JP: I would tell you that it is by law. With the RGPD / LOPD, Organic Law on Data Protection in the case of Spain. That law that was entered in 1998/2000 means that data cannot be shared, and I will give you an example. This law does not come from Spain, this law comes from Europe, but Spain added a small extra text. Spanish law states that data cannot be shared except for political parties, who can get your data.

JR: Indeed, and private companies that have a registered office or main headquarters are abroad, they can also commercialize the data they obtain through their applications.

Returning to why it is so difficult to implement a single Cloud. One of the main obstacles is cost. Because doing the program itself, the Framework, and all the work behind it, would not have a very exorbitant cost, but the unification of the data and the migration of these. There is a very, very high amount of money investment.

JP: Also, another drawback is that you must standardize the data, what do I mean by this; that one administration may put you "Spain", the other "Espanhol" and the other "Spanish" or "SP".

Regarding data, integrity is that usually each Country/Administration pulls its own, which is what always happens.

JR: And then not only that, but you also must consider that there are fewer and fewer outpatient clinics, medical centers, or other areas of the administration that

still work on paper. So going from paper to digitization is one step but going from paper to Cloud is a bigger step still.

In other words, we have a legislative factor, an economic factor, a material factor, let's say, of infrastructure, and at the level of management of each State of each autonomy.

I see a problem with this, you limit it by countries that each country has, apply its laws, its restrictions, etc. But the issue comes when a request comes from abroad to your country.

Imagine that you have everything mounted in the cloud. You work worldwide, everything on this same cloud, everything is unified, everything perfect in the ideal world and you go on a trip, any problem happens to you and from Italy, they send a request to Spain.

Let's put it that Italian health laws are more flexible than those in Spain. Once the solution is applied and they will unify the data. Which is the worth one? that of Italy or that of Spain, because you nationally belong to Spain, but you have been treated in Italy. So, what has more weight, where has it been treated or the laws that you say or where were you born? Here comes one of the first concerns.

Regarding Q4 these are the following answers:

JR: I wanted to propose two things regarding the Framework that we have. The request I understand that from Cloud 1 that requests a data or whatever Cloud 2, and Cloud 1 would receive this data.

And why not? Let Cloud 1 send the request and Cloud 2 give it access. On that Cloud two at the requester of the data and the data does not move.

Let me explain myself. The request is a pipe between clouds, I need this information and is like if you were going to the library to read a book, I need such a book and the librarian tells you, we have this book, you can read it, but you can't take it with you, you must read it here (Cloud providing the information).

In case they do not have it, that a request is created to request this data when the data is available. Returns that availability notifying the requester. Later, the request for the data visualization is automatically repeated and access is given to the visualization of that data when it is available. Finally, the end-user can visualize the information on-cloud premises.

Perse. Instead of data traveling, as it is going to be sensitive information that the information that depends on the region, community, or nation stays located at the cloud owner of that information. (In order not to avoid that there is so much transformation of the data involved and that then ends in that way and there is the inconsistency of data that can be given) this way is a request to access this data on-premises.

Then, Cloud two assesses if the "request" is real because it is a verified user, then end-to-end encryption is accepted. It is verified that everything is correct, it gives

access to the data and in case of not having the data, a "request" of that data is made, and a request is sent back once the data is available.

This is just one of the proposals, if it suits you, if not, that is, I see your approach well proposed. My suggestion is another additional alternative that you can have and that is also interesting and is usually used when there is sensitive information to issue/deliver. It is more common for them to enable you to see the data they send you precisely because it saves a lot of encryption and development procedures.

JP: In addition to this, a double validation both in Cloud 1 and Cloud 2. Let me explain, a double validation of what I am asking for is correct. And in Cloud 2 once it reaches the "request" and it is decrypted to verify what is being requested, it is something coherent and it is not asking us for something that is not expected.

Why the double-check? What happens if a “request” is sent, and while the “request” is being sent, the connection between Cloud 1 and Cloud 2 is lost. And for example, only half a “request” reaches Cloud 2.

Do we only return half the information? It would not make sense. The logic is to return entirely the requested information. In case the request is halfway through, a notification is triggered about the content that has arrived halfway, and it is verified: Is this how the data is wanted? An alert and double-check.

JP: Another suggestion. It is if there is a large volume of requests and information is expected. Make a load distribution having the Cloud replicated. For instance, Cloud 2A and Cloud 2B with the same data inside the Cloud 2 environment. This way, with a Framework in front that says that the first request for Cloud 2A, the second for Cloud 2B, etc. will avoid saturation in communications. Also, if one of the replicated Clouds drops communication, the Framework can detect that the sub-Cloud has fallen and re-drives the requests to a "backup" sub-Cloud.

This means more data availability and it also carries a security part since you have the data replicated, that is, it is more difficult to lose it.

JR: As per operational level, everything remains the same, your diagram should be the same, the flow is the same, the only thing is that there is a prior agent who is going to be the distributor, that is, within what would be the diagram that you painted what you can do is put sub-clouds with a distributor just below. A global operation of what would be the cloud as a whole and its clouds. In this way, we would optimize the process of requests between Clouds, which are also things to consider.

6. CONCLUSION

By the end of this dissertation, this chapter reflects the most relevant conclusions, constraints, and future work regarding public clouds interoperability within different administrations. It provides a different perspective and understanding of what are the main constraints that the European Union will face by integrating their institutions into one single public cloud as GAIA's X project aims.

Therefore, and considering the insights collected during the evaluation phase, we can verify that the original objectives have been met and that the proposed device can ensure the awareness and relevant considerations to implement and standardized process compatible between public clouds.

6.1 RESUME OF THE DEVELOPED WORK.

During the procedures of the investigation done on the different infrastructures, standards, and application of the Cloud within public environments. By gathering and constructing a solid literature review of the available information, the final artifact could be represented, discussed, and validated by two experts on Cloud Computing and Cloud Solutions.

6.2 CONSTRAINS

In the process of developing this paper, there were some limitations regarding the availability of infrastructures, laws, and information from improving the consistency format and sovereignty of the data that can be shared between clouds since there's no effective legislation that regulates in a unified way the methodology to operate. Each public administration relies now on different levels of capabilities.

To not extend the Cloud strategies from countries abroad of the European Union (EU). The adopted standards are currently the ones that suit the GDPR and international agreements on the European organizations that could be extrapolated individually to each country, region, or community (European Commission, Shaping Europe's digital future, 2020).

Also, the steps of the different stages previously scheduled were not fulfilled since there were divergences on the approach that the final artifact should suggest. As a result, the development of the final framework had to be redesigned on several occasions to suit the available technologies available and legislations from the European Union (European Commission, Communication from the commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions, 2020). By analyzing the structure of public organization Cloud services inside a specific country and its homolog on another administration, the framework could provide a wider angle of how the artifact proposed might impact positively the citizens who can get, social, economic, and healthcare advantages by having their information available and secure between institutions.

It is important to note that nowadays the technologies are on their exponential path of growth and most of the time they are ahead of the legislative regulations that

governments can deploy to standardize the form of usage of these technologies once they are applicable.

6.3 FUTURE WORK

This paper has settled the current paradigm of Cloud Computing Services within public administrations as a start point of administrations' digitalization. By harmonizing the regulations into a common benefit of services on the Cloud, both citizens and governments can develop a large system to dynamize their social, economic, and governance growth above their data.

Considering the continuous improvement of technologies, this framework and standards developed in this paper must be on continuous review. Also, this will contribute to consolidating a reference model that might help administrations to follow a path and work methodology to speed up any digital transition.

Finally, by the research done, this academic dissertation can help any other investigators to contextualize and arise new investigations based on what is being studied.

REFERENCES:

(BMWi), F. M. (2020). *Project GAIA-X a Federated Data Infrastructure.* Munich: Public Relations Division.

Ahmed Taha, R. T. (2017). *A Framework for Ranking Cloud Security Services.* Madrid: Technische Universität Dermstadt.

Bernard Le Masson. (2014). *Digital Government Pathways to Delivering Public Services for the Future.* London: Accenture.

Chastanet, P. (2019, December 12). *Shaping Europe's digital future*. Retrieved from Cloud and Software (Unit E.2): https://ec.europa.eu/digital-single-market/en/content/cloud-and-software-unit-e2

Cloud Select Industry Group on Service Level;. (2018). *ec.europa.* Retrieved from European Commission: https://ec.europa.eu/digital-single-market/en/cloud-select- industry-group-service-level-agreements

Code, C. S. (September 2018). *ec.europa.* Retrieved from European Commission: https://ec.europa.eu/digital-single-market/en/cloud-select- industry-group-code-conduct

Contracts, E. G. (2018). *ec.europa.* Retrieved from European Commission: http://ec.europa.eu/justice/contract/cloud-computing/expert- group/index en.htm

CTIC. (2020). *Estratégia Cloud para a Administração Pública em Portugal.* Lisboa: Concelho para as Tecnologias de Informação e Comunicação.

Economic, G. F. (2020). *GAIA-X: Policy Rules and Architecture of Standards.* Munich: Federal Ministry for Economic Affairs and Energy Public, Relations Division.

European Commission, E. (2020, February 19). Communication from the commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions. *A European Strategy for Data*. Brussels, Belgium: European Commission.

European Commission, E. (2020, Abril 20). *Shaping Europe's digital future*. Retrieved from European Comission: https://ec.europa.eu/digital-single-market/en/policies/cloud-computing

Fang Liu, J. T. (2011). *NIST Cloud Computing Reference Architecture.* Gaithersburg: National Institute of Standards and Technology.

GDPR. (2016). *European Commission.* Retrieved from Access to European Union Law: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

Gorelik, E. (2013). *Cloud Computing Models, Comparison of Cloud Computing Service and Deployment Models.* Massachusstes: Massachussets Institute of Technology.

Jonathan Roy, H. T. (2017). On the Use of ISO/IEC Standards to Address Data Quality Aspects in Big Data Analytics Cloud Services. *On the Use of ISO/IEC Standards* (pp. 2-7). Montreal : E´cole de technologie sup´erieure, Montreal QC, CAN .

Marek Moravik, P. S. (2018). *Overview of Cloud Computing Standards.* Retrieved 04 2020, from Research Gate: https://www.researchgate.net/publication/329645064

Ministerio de Asuntos Econòmicos y Transformación Digital. (2020). *Plan España Digital 2025.* Madrid: Gobierno de España.

Mohammed Alhamad, T. D. (2010). Conceptual SLA Framwork for Cloud Comupting. *Digital Ecosystems and Business Intelligence Institute (DEBII)*, 1-3.

NIST. (2011). *Published, Final Version of NIST Cloud Computing Definition.* Retrieved from Technology's, National Institute of Standards and: https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published

Nunes, F. (2020). *Portuguesa IP Telecom junta-se à "cloud" europeia Gaia-X.* Retrieved from Sapo: https://eco.sapo.pt/

Prof. Alan R. Hevner, P. (2004, March 23). Design Science in Information systems Research. *Mis Quarterly*, p. 33.

Prof. Alan R. Hevner, P. (2018, June 18). Design Science. (P. D. Winter, Interviewer)

Scott Dowell, A. B. (2014). *Cloud to Cloud Interoperability.* San Diego: Computer Science Corporation.

Sean Carlin, K. C. (2012, June 5). Cloud Computing Technologies. *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*, p. 7.

Silva, M. (2007). Redes de petri continuas: Expresividad, análisis y control de una clase de sistemas lineales conmutados. *Revista Iberoamericana de Automática e Informática Industrial*, 8-15.

Smart Cities, S. (2017, January 20). Nasceu o cluster Smart Cities Portugal. *Smart Cities*, p. 1.

The European Commission, o. s. (2013). *European Commission.* Retrieved 23 2020, from Expert group on cloud computing contracts: https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/cloud-computing/expert-group-cloud-computing-contracts_en

APPENDIXES

APENDIX 1: GAIA X Project Requirements

TOPIC	POLICY RULE	Included in the description of the service (Machine Readable)	Mandatory or Optional	Validation Mechanism : Self declaration or Third Party certified (may be through a Code of Conduct)	Tool	Comment
	RULES TO BE APPLIED TO THE PROVIDER					
POLICY	Public declaration of Adherence to the principles set out in Art. 6 of the Free Flow of Data Regulation of the European Union	Yes	Mandatory	Self Declaration	URL	
	The cloud provider shall regularly review the implementation of all GAIA-X Policy Rules examined in this catalogue in an internal audit procedure. For this purpose, the cloud provider defines control procedures and responsibilities.	No	Mandatory	Self Declaration or Third Party certified		
	At least one service declared, once GAIA-X in production phase.	No	Mandatory	Self Declaration or Third Party certified		
POLICY	Portability of licences: floating licences available in the same conditions than pay as you go model.	No	Mandatory	Self Declaration		
	RULES TO BE APPLIED TO THE SERVICE (INFRASTRUCTURE)					
LOCATION	Ability to choose data stored and processed within EU/EEA	Yes	Mandotory	Third Party Certified	CISPE Data Protection Code of Conduct	
LOCATION	Transparency Non-EU Applicable Extraterritorial Regulations	Yes	Mandotory	Self Declaration		Detailed list to be machine readable: Cloud Act, Patriot Act, China...
CONTRACT	No access to customer data by Cloud Infrastructure Provider, unless specifically authorized by the customer	Yes	Mandotory	Third Party Certified	CISPE Data Protection Code of Conduct	
SECURITY	European Cloud Security Certification - High or equivalent	Yes	Optional	Third Party Certified	ENISA Guidance (SecNumCloud ? C5 ?)	A list of equivalent Information security certifications/ attestations will be compiled and will follow the guidance of the ENISA
SECURITY	European Cloud Security Certification - Substantial or equivalent	Yes	Optional	Third Party Certified	ENISA Guidance (SecNumCloud ? C5 ?)	
SECURITY	European Cloud Security Certification - Basic or equivalent	Yes	Mandotory	Self declaration* (to be checked by independant Monitoring Body)	ENISA Guidance	
CONTRACT	The infrastructure cloud provider ensures, with appropriate technical or organisational precautions, that the cloud service is only provided after the conclusion of a legally binding contract with the cloud user.	No	Mandatory	Self Declaration or Third Party certified		
CONTRACT	The contract between the infrastructure cloud service provider and the cloud user clearly defines the respective role and shared responsibilities of the cloud provider and the cloud user with respect to security and data protection compliance as well as the technical config-uration of the environment.	No	Mandatory	Self Declaration or Third Party certified		
CONTRACT	The contract between infrastructure cloud provider and data controller falls under the jurisdiction of an EU member state	Yes	Mandatory	Self Declaration or Third Party certified		
CONTRACT	The legally binding contract provides that all data will only be processed upon documented instruction by the cloud user	No	Mandatory	Self Declaration or Third Party certified		
DATA PROTECTION	Where the cloud user uses cloud services to process personal data, the infrastructure cloud provider is a processor that shall comply with all obligations applicable to processors under GDPR.	No	Mandatory for services processing PII	–	CISPE Data Protection Code of Conduct	
DATA PROTECTION	The cloud provider shall not process cloud user personal data for data mining, profiling or marketing pruposes nor for accessing such cloud user personal data unless if it is necessary to provide the cloud sevices.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider ensures that the processing of the cloud user's personal data is only carried out on the cloud user's instructions in accordance with the processing agreement.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider shall provide the cloud user with privacy, security, design and management information, in order to enable the cloud user to perform security and data protection impact assessments.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		

TOPIC	POLICY RULE	Included in the description of the service (Machine Readable)	Mandatory or Optional	Validation Mechanism : Self declaration or Third Party certified (may be through a Code of Conduct)	Tool	Comment
DATA PROTECTION	For cloud services offering the possibilily for the data to be processed in different locations outside of the EEA and unless such data are only routed through such locations, the circum-stances of the transfer and appropriate safeguard shall be set out in the agreement entered into between the cloud user and the infrastructure cloud provider.	Yes	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider ensures, with appropriate measures, that the cloud user has the opportunity to carry out the rectification and completion of personal data itself, or have it carried out by the infrastructure cloud provider.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider ensures that the cloud user has the opportunity to carry out the erasure of personal data itself, or have it carried out by the cloud provider.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider ensures that the cloud user has the opportunity to restrict the processing of personal data itself, or have the restriction carried out by the cloud provider.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	Where the infrastructure cloud provider is obligated to designate a data protection officer (DPO), it shall appoint one on the basis of professional qualities and expert knowledge of data protection law and practices, as well as on the basis of the ability to fulfil the tasks referred to in Article 39 GDPR	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider shall require an independent and external third party to regularly control the compliance of the cloud provider with these data protection requirements.	Yes	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider ensures by the application of appropriate technical or organisational measures the confidentiality, veracity and availability of the data of the controller. Risk appropriate transfer encryptiono. Traceability of data processingo. Separate processingo. Restorabilty after incidentso ...	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider ensures that a cloud service is only provided with the inclusion of sub-processors processing cloud user's data, if and to the extent that the cloud user has agreed to this sub-processing beforehand in the contract.	Yes	Mandatory for services processing PII	Self Declaration or Third Party certified		
SUB-PROCESSOR	The infrastructure cloud provider ensures that its sub-processors only act on the basis of a legally binding sub-processing agreement that is in accordance with the contract entered into between the cloud provider and cloud user.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
SUB-PROCESSOR	The infrastructure cloud provider informs the cloud user about the identity of all sub-processors processing the cloud user's data it involves at all levels as well as of any intended change of such sub-proccessors.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
REPORTING	The infrastructure cloud provider must notify the cloud user immediately in the event in which, during the period of validity of the contract the location of data processing changes from the one specified in the agreement for reasons in the area of responsibility of the cloud provider	No	Optional	Self Declaration or Third Party certified		
REPORTING	The infrastructure cloud provider ensures, with appropriate measures, that it notifies personal data breaches and their extent to the cloud user without undue delay.	No	Mandatory	Self Declaration or Third Party certified		
REPORTING	The infrastructure cloud provider shall maintain a record of processing activities composed of the information it has visibility on.	No	Mandatory	Self Declaration or Third Party certified		
REVERSIBILITY	Adherence to the principles of porting of data as described in Art. 6 of the Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IaaS Code of Conduct; https://swipo.eu	

TOPIC	POLICY RULE	Included in the description of the service (Machine Readable)	Mandatory or Optional	Validation Mechanism : Self declaration or Third Party certified (may be through a Code of Conduct)	Tool	Comment
	RULES TO BE APPLIED TO THE PROVIDER					
POLICY	Public declaration of Adherence to the principles set out in Art. 6 of the Free Flow of Data Regulation of the European Union	Yes	Mandatory	Self Declaration	URL	
POLICY	The cloud provider shall regularly review the implementation of all GAIA-X Policy Rules examined in this catalogue in an internal audit procedure. For this purpose, the cloud provider defines control procedures and responsibilities.	No	Mandatory	Self Declaration or Third Party certified		
POLICY	At least one service declared, once GAIA-X in production phase.	No	Mandatory	Self Declaration or Third Party certified		
POLICY	Portability of licences: floating licences available in the same conditions than pay as you go model.	No	Mandatory	Self Declaration		
	RULES TO BE APPLIED TO THE SERVICE (INFRASTRUCTURE)					
LOCATION	Ability to choose data stored and processed within EU/EEA		Mandatory	Third Party Certified	CISPE Data Protection Code of Conduct	
LOCATION	Transparency Non-EU Applicable Extraterritorial Regulations		Mandatory	Self Declaration		Detailed list to be machine readable: Cloud Act, Patriot Act, China...
SECURITY	European Cloud Security Certification – High		Optional	Third Party Certified	ENISA Guidance (SecNumCloud ? C5 ?)	Decision to be made, once the ENISA output is clear based on the Cybsercurity Act. Tansition mechanism (SecNum Cloud and/or C5) to be agreed until ENISA scheme made public.
SECURITY	European Cloud Security Certification – Substantial		Optional	Third Party Certified	ENISA Guidance (SecNumCloud ? C5 ?)	
SECURITY	European Cloud Security Certification – Basic		Mandatory	Self declaration* (to be checked by independant Monitoring Body)	ENISA Guidance	
REVERSIBILITY	Adherence to the principles of porting of data as described in Art. 6 of the Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO SaaS Code of Conduct; https://swipo.eu	
GDPR CONTRACT	The infrastructure cloud provider ensures, with appropriate technical or organisational precautions, that the cloud service is only provided after the conclusion of a legally binding contract with the cloud user.		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR CONTRACT	The contract between the infrastructure cloud service provider and the cloud user clearly defines the respective role and shared responsibilities of the cloud provider and the cloud user with respect to security and data protection compliance as well as the technical configuration of the environment.		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR CONTRACT	The contract between infrastructure cloud provider and data controller falls under the jurisdiction of an EU member state		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR CONTRACT	The legally binding contract provides that all data will only be processed upon documented instruction by the cloud user		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider shall not process cloud user personal data for data mining, profiling or marketing purposes nor for accessing such cloud user personal data unless if it is necessary to provide the cloud sevices.		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The contract between CSP and data controller falls under the jurisdiction of an EU member state		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The subject-matter and the duration of the processing must be outlined as specifically as possible in the legally binding agreement on the order processing		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The legally binding data processing agreement provides that all data will only be processed upon documented instruction by the controller		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	

TOPIC	POLICY RULE	Included in the description of the service (Machine Readable)	Mandatory or Optional	Validation Mechanism : Self declaration or Third Party certified (may be through a Code of Conduct)	Tool	Comment
GDPR DATA PROTECTION	The cloud provider ensures by the application of appropriate technical or organisational measures the confidentiality, veracity and availability of the data of the controller		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures that the processing of the cloud user's data is only carried out on the cloud user's instructions		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The obligations of the cloud provider to return data media, return data and erase data after the end of the data processing must be set out in a legally binding order processing agree-ment		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures that a cloud service is only provided with the inclusion of sub-processors, if and to the extent that the cloud user has agreed to this sub-processing beforehand in writing or text form.		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures that its sub-processors only act on the basis of a legally binding sub-processing agreement that is in accordance with the legally binding processing agreement between the cloud provider and cloud user		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider informs the cloud user about the identity of all sub-processors it involves at all levels		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The obligations of the cloud provider to return data media, return data and erase data after the end of the data processing must be set out in a legally binding order processing agreement		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider must notify the cloud user immediately in the event in which, during the period of validity of the agreement, the place of data processing changes from the one specified in the agreement for reasons in the area of responsibility of the cloud provider		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures, with appropriate measures, that it notifies personal data breaches and their extent to the cloud user without undue delay		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider shall maintain a up-to-date record of processing activities		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures that the cloud user has the opportunity to provide data subjects with information about the data processing and give them a copy of the personal data, or arrange this via the cloud provider.		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures, with appropriate measures, that the cloud user has the opportunity to carry out the rectification and completion of personal data itself, or have it carried out by the cloud provider		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures that the cloud user has the opportunity to carry out the erasure of personal data itself, or have it carried out by the cloud provider		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures that the cloud user has the opportunity to restrict the processing of personal data itself, or have the restriction carried out by the cloud provider		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	Where the cloud provider is obligated to designate a data protection officer (DPO), it shall appoint one on the basis of professional qualities and expert knowledge of data protection law and practices, as well as on the basis of the ability to fulfil the tasks referred to in Article 39 GDPR		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider shall only process the cloud user's personal data where this is required to achieve the specified purposes of the processing		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures that the cloud user has the opportunity to transmit the personal data provided by a data subject to this person or another controller in a structured, commonly used and machine-readable format, or have it transmitted by the cloud provider		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider assists the cloud user in the execution of its data protection impact assessment. If the cloud provider is aware of a high risk of processing due to a data protection impact assessment carried out beforehand by the cloud user, the cloud provider must take risk-appropriate precautions.		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
DATA SHARING	The components used for sharing data shall provide a sufficiently high degree of trust and security regarding the in-tegrity, confidentiality and availability of information exchanged.	Yes	Mandatory	Third Party certified	DIN SPEC 27070	

TOPIC	POLICY RULE	Included in the description of the service (Machine Readable)	Mandatory or Optional	Validation Mechanism : Self declaration or Third Party certified (may be through a Code of Conduct)	Tool	Comment
DATA SHARING	The components used for sharing data allow each other to check integrity of each other's software stack via remote attestation.	Yes	Mandatory		DIN SPEC 27070	
DATA SHARING	The components used for sharing data allow data providers to define usage policies that will be published together with the data offered.	Yes	Mandatory	Third Party certified	DIN SPEC 27070	
DATA SHARING	Components used for data sharing shall provide a self-description (i. e. metadata) via a defined interface.	Yes	Mandatory	Self Declaration	DIN SPEC 27070	
	Components used for data sharing offering data send usage policy to be applied to components requesting data every time connection is established.	Yes	Mandatory		DIN SPEC 27070	
DATA SHARING	The components used for sharing data shall facilitate technical enforcement of data usage policy specified.	Yes	Mandatory	Third Party certified	DIN SPEC 27070	
DATA SHARING	The administrators of the data provider side cannot change rules regarding data flow without data provider taking notice of the change and approving it.	Yes	Mandatory	Third Party certified	DIN SPEC 27070	
DATA SHARING	The components used for sharing data verify authenticity and integrity of all system components prior to execution.	Yes	Mandatory	Third Party certified	DIN SPEC 27070	
DATA SHARING	The components used for data sharing shall log each access control decision, every access to data, any changes made to its configuration and every case in which a service receives fewer resources than requested in the form of an integrity protected log entry in its domain.	Yes	Mandatory	Third Party certified	DIN SPEC 27070	
DATA SHARING	The data consumer and provider shall identify its organization via unified digital identities.	Yes	Mandatory	Third Party certified	eIDAS regulation Nr. 910/2014	
DATA SHARING	The data consumer and provider shall identify the components used for data sharing and processing via unified digital identities.	Yes	Mandatory	Third Party certified	eIDAS regulation Nr. 910/2014	

ANNEXES

Experts Interviews.

Interviews' transcription concerning the projected core' objective of the framework proposed and stage of the thesis.

To rigidly respect the original declaration of the interviewees, the following document is expressed with the native language of the experts.

1. Experts on Banking & CRM Cloud Services & Solutions.

Date: Sunday, 10th October 2021.

Location: Skype Meeting.

Introduction & biography of Juan Payeras:

Soy Juan Payeras soy de Mallorca. He estudiado el grado de ingeniería informática y actualmente estoy trabajando en el CRM de Iberostar de Project Manager, es decir, de dirección de proyectos. Un poco mi currículum, llevo desde 2019 trabajando en el CRM de Iberostar, pero también había hecho prácticas en BI tanto en Iberostar como en Meliá Co.

Moderator: ¿Cuál es tu experiencia con Cloud Computing? ¿Cuál ha sido tu trabajo o interactividad que tienes con la nube?

Juan: En el CRM estamos trabajando diariamente con Cloud. Utilizamos una herramienta que se llama SalesForce, que en teoría es el CRM número 1 qué hay actualmente en el mercado y todo lo que hacemos siempre está en Cloud, tiene una lógica muy similar a lo que intentas hacer tú. Por eso creo que tanto José Ramón y yo podemos darte una visión que puede ser bastante interesante.

Introduction & biography of José Ramón Redondo Espinosa:

Soy José Ramón Redondo Espinosa trabajo actualmente en Eberis que es una consultoría como desarrollador, analista técnico y funcional. Tengo estudios superiores como desarrollador de aplicaciones Multiplataforma y tengo una licenciatura como Cloud Solution en SalesForce. Principalmente he estado en proyectos tanto de banca como inmobiliaria, como de Industria, Farma, para la implementación de soluciones en la nube. Ya sea a través de SalesForce, ViVa u otros CRM propios desarrollados por el cliente. Mi aportación es una visión muy técnica en los proyectos, más que en el funcionamiento, aunque también he desarrollado análisis de la parte funcional.

Moderator: Me gustaría validar el Framework desarrollado para la interoperabilidad entre dos Clouds. Nos centraremos en dos Clouds de dominio Público y estaría

interesado en evaluar el esquema presentado para entender cuáles serían "*constrains*" que nos encontraríamos en el proceso de flujo de información entre nubes y los puntos críticos para tener en cuenta estandarizar de forma segura la información entre varias administraciones que usan el Cloud.

Como habíamos analizado en la reunión anterior, comentamos que hay una llave pública y otra privada entre Clouds. ¿Podríais desarrollar los conceptos?

José Ramón: Bueno, en un principio sería un cifrado de extremo a extremo, tanto en lo que sería la "*request*" como la información recibida, de forma que esté cifrado de extremo a extremo se haría con dos llaves. Una llave pública que tendría tanto el usuario que está emitiendo el "*request"* como la propia Cloud receptora, que sería la misma llave.

Luego una llave privada que la generaría quién está emitiendo la "*request"* y el propio servidor Cloud. De este modo, sin meternos en mucho detalle técnico, una vez que el usuario cifra su petición con los datos que esté pidiendo, tendrá en un extremo la llave privada y en el otro la llave pública.

Una vez que la recibe el servidor, con su llave privada. Sería capaz de desbloquear este cifrado y obtener la información de la petición. Tras las validaciones necesarias en esta petición, devolvería una respuesta cifrada de igual modo. El usuario la recibiría y la descifraría de igual manera que se descifra en el servidor.

Moderator: ¿Una duda que os hago para incluso mejorar este Framework referente a la primera pregunta es, creéis que la solicitud también tiene que ir a encriptada aparte del dato que hay que enviar?

José Ramón: Yo creo que sí debería de ir a encriptado y te explico el por qué. Porque muchas veces las fugas de datos se suelen dar por esa petición. Si tú mandas una petición sin cifrar puede darse que esa información, llegue a las de un agente externo que pueda sepa el dato requerido y lo emita obteniendo la información de forma fraudulenta a cambio.

Por otro lado, si la petición está cifrada. Aunque obtenga la petición, como no va a disponer de la clave privada que utiliza la nube para descifrar, no podría hacer ningún tipo de inyección de datos o de código o cualquier otra fisura o vulnerabilidad que se diera en el servicio.

Juan: Correcto. Nosotros, por ejemplo, en Iberostar lo que hacemos con la información de pago, es que, no la guardamos. Por ejemplo, información de pagos con tarjetas de crédito e informaciones relacionadas. En cambio, una cosa que guardamos ya que tenemos la página web, son las cuentas de los usuarios qué tienen una "*password"*.

La "*password"* se encripta al origen por seguridad, en el supuesto que

hubiese alguien que quisiera interceptar la comunicación. No pudiese averiguar la *password* de ese cliente y poder ver información a personal o sensible

Moderator: A nivel de seguridad, es decir, de encriptación. ¿Seguís algún estándar? ¿Es decir, tenéis un proceso que diga el "*step by step*" específico que fijen la seguridad de los datos que se envían y se reciben?

José Ramón: Depende un poco de y hacia dónde queramos ir. Tenemos la opción 1 que sería si queremos guardar todo. Si queremos guardar todos los datos que recibimos. En ese caso lo más seguro y lo que seguramente seguirá las normativas va a ser hacer un cifrado completo de todo el Cloud y su información. El pro es que se convierte en una información muy segura. El contra que tiene es la optimización.

Ralentizaría un poco el flujo de datos, aunque tampoco tendría un impacto muy grande, pero si ralentizara las peticiones de datos. El tener que encriptarse, mandarse, des-encriptarse, responder a la petición, volverla a encriptar y des-encriptarla otra vez. Este sería el camino si esa información la queremos conservar.

La segunda opción o camino sería sí, únicamente va a ser necesaria la información durante la petición y solamente mantenerla viva durante la petición y que luego esa información no se almacene ningún sitio. Se elimina, desaparece, se pierda, se quede en la nada.

De este segundo tipo, pues podremos tener, como por ejemplo para entender este concepto, una base de nombre, una base de datos donde tengamos todos los nombres y DNIs de gente.

Por ejemplo, recibimos una petición de información que necesitamos saber de un Cloud para otro. El DNI de X persona en este caso no nos haría falta guardar los datos de la persona, haríamos visible el dato existente únicamente mientras se está haciendo la petición. entonces aquí verdaderamente no haría falta hacer un cifrado completo, ya que una vez que la petición muere y ya está la respuesta a la petición, tanto la información (dato) cómo la petición deja de existir. Entonces no hay posibilidad, ni ninguna probabilidad en la que en la que se pueda producir una fuga de datos.

Moderator: ¿A nivel de riesgos, ¿cuáles son los riesgos más comunes que os encontráis cuando transferís o migráis datos de un lugar a otro?

Juan: El riesgo más común siempre es el error humano. Es decir, por mucha seguridad que pongas, si el humano falla, el sistema puede estar lo bien hecho que quieras, que va a fallar.

Te pongo un caso práctico. En Iberostar tenemos, así, como he comentado, tenemos los huéspedes o la gente que entra en Iberostar. Qué pasa, muchas veces tenemos un mecanismo de fusión de clientes por X o por Y, sabemos que son el mismo cliente.

Si el "*Call Center*" o los agentes del "*Call Center*" se equivocan, se equivocan. Por una mala praxis, fusionando los clientes que no toca ese ya no se puede recuperar. Porque desaparece. Eso, por ejemplo, es un error humano que nosotros no podemos controlar.

Nosotros les damos las herramientas, ponemos ciertas limitaciones a esas herramientas, pero un mal uso, siempre es el típico error que puede generar problemas.

José Ramón: Otro error muy común, que se suele producir suele ser durante las cargas de datos durante las carreras masivas de datos, ya sean en la nube, en un servidor propio. Malas prácticas, falta de seguridad o protocolos, puede generar que esos datos que migramos terminen quedándose en el dispositivo de quien hace la carga en local o que se olviden de cargarse los archivos y terminan en manos de quien no debe, etcétera. Estos suelen ser los errores más comunes y las faltas que se suelen ver en el día a día.

Moderator: ¿Existe algún indicador, métrica o SLA que detecte los errores en seguridad que tenéis?

Juan: SalesForce lo que tiene es a pagando un extra. Digámoslo así, por volumen de datos, te encripta los datos. Que quiere decir. Sí tú intentas acceder a esos datos encriptados. SalesForce se encarga de esa seguridad, o la herramienta contratada.

En nuestro caso no nos encargamos nosotros, de lo que sí que nos encargamos es, por ejemplo, a encriptar la contraseña en origen y guardarla encriptada en destino, que sería el CRM en este caso. Seguridad en sí. El que pone mayor seguridad por un lado en el CRM es SalesForce, y por otro lado, en los servicios que tenemos de las máquinas virtuales es el equipo de IT. El equipo de IT y de sistemas.

José Ramón: Es que aquí la vulnerabilidad la hay que abordarla, tanto por lo que puede dar el propio software, por su desarrollo, su estructura, su arquitectura, como a través del hardware, ya sean dispositivos externos, tipo USB, una impresora, un fax, un teléfono fijo. Cualquier dispositivo que esté en lo que sería la red o directamente conectado a cualquier dispositivo se encuentre dentro de red, es una vulnerabilidad de hardware. Qué se pueden encontrar los infectados, pueden ser un punto de acceso o cualquier cosa similar y luego están las vulnerabilidades del software, que puede ser porque tenga una estructura que no siga un flujo restringido donde tenga un origen y un fin las peticiones y no haya ninguna opción a que a que se quede en un bucle infinito mandando una respuesta hasta el infinito y más allá. O ya sea a nivel de arquitectura, porque no se defina bien, que se tiene que quedar encriptado, que es útil quedarse y que no etc.

Entiendo por tanto que hay una parte de responsabilidad del proveedor del Cloud y otra parte responsabilidad del consumidor como cliente.

Otro protocolo de seguridad o que te obliga SalesForce es que nosotros desarrollamos a peticiones SOAP. Al contrario que las peticiones REST, las peticiones SOAP te obligan a identificarte.

Es decir, antes de poder proceder, con una recuperación de datos, tienes que identificarte de esta forma se me otorga un identificador. Cuando me pasas el identificador, luego puedo pedir la información. Es una forma de saber quién eres antes para pasarte los datos.

Moderator: ¿A que nos referimos cuando hablamos de peticiones REST y SOAP?

Juan + José Ramón: Las peticiones REST normalmente no requiere una identificación. REST a nivel técnico, un documento de texto plano como puede ser un *".txt"*, le pones la extensión. HTML, y le puedes añadir una petición de mándame las cuentas necesarias y REST te las va a devolver.

Moderator: ¿Cómo se suelen proteger las peticiones REST?

José Ramón + Juan: Estuve en un proyecto donde, sí, desarrollamos esto un sistema para proteger peticiones REST. Esto como se suele proteger es con un inicio previo de sesión. Con una cuenta de usuario que se debe dar de alta y depende del organismo que contrate la Aplicación o App. Y la REST únicamente se solicita a la red y devuelve la información.

A la hora de hacer una petición de información que sea confidencial, por ejemplo, historiales médicos, documentación sensible no se suele hacer nunca una petición REST.

Información sensible se suele hacer con petición SOAP para que quede registrado quién está mandando esta petición. En caso de que se cometa un fraude, un delito o lo que sea, se pueda identificar quien fue el autor de la petición.

Para una interoperabilidad entre dos administraciones que usan Cloud, se trataría de información sensible, por lo tanto, siempre sería más seguro tirar por peticiones o SOAP.

Peticiones REST en el uso diario se suele ver es cuando, por ejemplo, una compañía tiene dispositivos que van a trabajar offline y dispositivos que están trabajando en la nube online entonces para sincronizar unos datos con otros, ahí si van a utilizar un REST, porque no hay posibilidad de fuga de datos porque se conecta todo en la misma red sin tener contacto exterior. En el caso que nos presentas ahora mismo planteado que son dos Clouds que sí que tiene comunicación al exterior, sería necesario tirar por el camino de peticiones SOAP que es el más restrictivo y seguro de la respuesta.

Moderator: Todavía hay mucha información que no está almacenada en Cloud, y están en una base de datos física poco accesible tanto para el ciudadano como para la administración. ¿Cuáles creéis que serían los beneficios de usar Cloud Computing entre países?

José Ramón + Juan: Pongamos un ejemplo que te va a responder a una parte de ello. Imagínate que soy de Madrid y me voy a Galicia, por ejemplo, y me rompo una pierna. Tengo un accidente. Que sería más práctico. Que avise mis datos al momento. O que me tuvieran que hacer la prueba de sangre es o inyectarme cero negativos, que es una sangre que va muy escasa.

Para cualquier administración tener los datos prácticamente al momento ganaríamos una rapidez en no tener que hacer pruebas o dos en poder gastar esa cero negativo en quien lo necesite y realmente.

José Ramón: Aquí haciendo un análisis un poco más a nivel de funcionamiento, tendríamos un impacto beneficioso, social. Además, tendría un impacto positivo a nivel económico, ya que. Esto requiere de un mantenimiento y requiere de un soporte y requiere de cosas, no que económicamente a quien lo propone le va a resultar beneficioso, al igual que a nivel social.

En adición, permite una diversificación de los datos, de forma que su accesibilidad más más útil. No, no pasa como actualmente pasa en España que si te tratas una enfermedad en una comunidad y te vas a otra. La otra comunidad no tiene los datos de la primera. Y no sabes si te has tratado de neumonía, si has Estado ingresado, si te ha pasado, vete a saber qué.

Entonces, esa diversidad de datos permite que por cada inquilino se tenga una sola una sola línea de información con todo su historial, sus cosas, etcétera.

De la otra forma, terminas teniendo 1000 líneas para una misma persona y vete a saber cuál es la que es correcta.

Moderator: **¿Por qué creéis que cuesta tanto poder implementar una compatibilidad o único Cloud para poder tener esa facilidad en compartir los datos o enviar datos a través de administraciones?**

Juan: Realmente te diría que es por la ley. Con la RGPD/LOPD, Ley Orgánica de Protección de Datos. Esa ley que entró en 1998/2000, más o menos, hace que no se puedan compartir datos y te voy a poner un ejemplo. Esta ley no viene de España, esta ley viene de Europa, España la íntegro. Y puso una letra pequeña. Y era. Que no se pueden compartir los datos a excepción de los partidos políticos, que sí que pueden conseguir tus datos.

José Ramón: Efectivamente, y las empresas privadas que tengan una sede social o sede principal está en el extranjero, también puede comercializar los datos que consiga a través de sus aplicaciones.

Volviendo al por qué es tan complicado implementar un Cloud único. Uno de los principales obstáculos es el costo. Por que realizar el programa en sí, el Framework y todo el trabajo que tenga por detrás, no tendría un costo muy desorbitado, pero la unificación de los datos y la migración de estos. Ahí sí que hay una cantidad de dinero muy, muy elevado.

Juan: Además, otro inconveniente es que tienes que estandarizar los datos, que te quiero decir con esto; que una administración a lo mejor te pondrá "España", en la otra "español" y el otra "Spanish" o "SP".

Hay estandarizar los datos. ¿Qué pasa? Cada comunidad/Administración tira a lo suyo, que es lo que siempre pasa.

José Ramón: Y luego no solo eso, sino que también hay que tener en cuenta que ya cada vez menos, pero todavía existen ambulatorios, centros médicos u otras áreas de la administración, que todavía trabajan a papel. Entonces, pasar del papel a la digitalización es un paso, pero pasar de papel a Cloud es un paso más grande todavía.

Moderator: O sea, tenemos un factor legislativo, un factor económico, un factor material, digamos, de infraestructura y también a nivel de gestión propia de cada Estado de cada autonomía.

Moderator: No sé si habéis escuchado hablar del proyecto GAIA X de la Unión Europea.

José Ramón: Algo me suena sí.

Moderator: Os explico un poco. El proyecto GAIA X es un proyecto que se empezó a desarrollar en Alemania y empezó como un clúster empresarial que se quiere extrapolar a la administración.

Lo que pretende es unificar o realizar un Cloud Europeo donde se facilite la transacción de datos como el flujo de información entre países de una forma segura, donde cada país tenga soberanía, encriptación, etc. sobre esos datos.

Es un proyecto que se está empezando a desarrollar, y se están empezando a hacer las primeras guías/directrices, para el objetivo final que es tener un espacio Cloud Europeo.

José Ramón: Sí, y claro, yo a esto le veo una pega, lo limitas por países que cada país tenga, aplique sus leyes, sus restricciones y lo que tenga que aplicar. Pero el tema viene cuando llega una petición del extranjero a tu país.

Imagínate que tienes todo montado en la nube. Trabajas a nivel mundial, todo sobre esta misma nube, todo está unificado, todo perfecto en el mundo idóneo y te vas de viaje, te sucede cualquier problema y desde Italia mandan una petición a España.

Pongámonos en que las leyes italianas en sanidad son más flexibles que las de España. Una vez que se aplica la solución y van a unificar los datos. ¿Cuál es la que vale? la de Italia o la de España, porque tú nacionalmente, perteneces a España, pero has sido tratado en Italia. ¿Entonces, qué tiene más peso, donde ha sido tratado o las leyes que dice tu ni dónde has nacido? Ahí viene una de las primeras preocupaciones.

José Ramón: Quería proponerte dos cosas respecto al Framework que tenemos. La petición entiendo que desde la Cloud 1 que pide un dato o lo que sea la Cloud 2 y la Cloud 1 recibiría este dato.

¿Y por qué no? Que la Cloud 1 mande la petición y la Cloud 2 le de acceso. Sobre esa Cloud dos a la petición del dato y que el dato no se mueva.

No sé si me explico, que la petición sea a modo de cómo si fuera una tubería. En plan, necesito este dato y como si fueras a la biblioteca a leer un libro, necesito tal libro y la bibliotecaria te dice, si mira aquí lo tienen, pero no se lo puede llevar usted, lo tiene que leer aquí.

En caso de que no lo tengan, que se cree un una recueste petición de ser solicitado este dato cuando el dato esté disponible. Devuelve esa disponibilidad como esta, OK, y automáticamente se repite la petición para la visualización del dato y se da acceso a la a la visualización de ese dato cuando esté cuando esté disponible. Y lo doy al usuario final para que lo visualice.

En sí. En vez de que un dato viaje, cómo va a ser información sensible que la Información que dependiendo de la región, comarca o nación donde se encuentre va a estar de una manera u otra (Para no evitar que haya de por medio tanta transformación del dato y que luego termine de aquella manera y exista inconsistencia de datos que se pueden dar) que sea una petición de acceder a este dato.

Entonces, Cloud dos valora si la "*request*" es real porque es un usuario verificado entonces se acepta el cifrado de extremo a extremo. Se comprueba que todo es correcto, da acceso al dato y en caso de no tener el dato se realice un "*request*" de ese dato y manda una solicitud de vuelta una vez que el dato esté disponible.

Esto es solo una de las propuestas, si te encaja, si no, o sea, yo este planteamiento, lo veo bien, el otro es otra alternativa adicional que puedes tener y que también está interesante y se suele utilizar cuando hay temas de información sensible. Es más común que te habiliten ver el dato a que te manden precisamente porque se ahorra mucho trámite de encriptación y desarrollo.

Adicionalmente a esto una doble validación tanto en la Cloud 1 y Cloud 2. Me explico, una doble validación de lo que estoy pidiendo es correcto. Y en el Cloud 2 una vez que

llegue a la "*request*" y se des-encripte que verifique qué es lo que se está pidiendo, es algo coherente y que no nos está pidiendo una cosa que no se espera.

¿Por qué la doble comprobación? Qué sucede si se manda una "*request*", y mientras se está generando el envío de la "*request*", se pierde la conexión entre Cloud 1 y Cloud 2. Y, por ejemplo, llega solamente media "request" a la Cloud 2.

¿Solamente devolvemos la mitad de información? No tendría sentido.

O se devuelve la petición entera. O en caso de que la petición esté a medias, que se dispare una notificación sobre el contenido que ha llegado a medias, y se verifique: ¿Es así como verdaderamente se quiere el dato? Una alerta, un doble check.

Juan: Otra sugerencia. Es si hay un volumen o se espera un volumen muy grande de peticiones e información. Hacer una distribución de carga, es decir, tener el Cloud replicado. Por ejemplo; **Cloud 2A** y **Cloud 2B** con los mismos datos. De esta forma con un Framework delante que diga que la primera petición para el Cloud 2ª, la segunda para el Cloud 2B etc. para evitar saturación en las comunicaciones. De esta forma, si uno de los Cloud replicados se cae la comunicación, el Framework lo puede detectar de que Cloud ha caído y desviar las peticiones a un Cloud de "*backup"*.

Esto significa más de disponibilidad de datos. Y también conlleva una parte de seguridad ya que tienes los datos replicados, es decir, es más difícil perderlos.

José Ramón: A nivel de funcionamiento que se mantiene todo exactamente igual, el diagrama es el mismo, el flujo es el mismo, la única cosa es que hay un agente previo que va a ser el distribuidor, es decir, dentro de lo que sería el diagrama que tú pintaste lo que puedes hacer es poner sub-nubes con un distribuidor justamente debajo. Un funcionamiento global de lo que sería la nube en conjunto y sus nubes. De esta forma optimizaríamos el proceso de peticiones entre Clouds que también son cosas que considerar.

Moderator: Muchas gracias por vuestras aportaciones a lo largo de esta entrevista. Os agradezco la asistencia y el tiempo dedicado. Hasta aquí nuestra evaluación de propuesta sobre interoperabilidad entre clouds.

Juan + José: Ramón: Muchas gracias.