InterPARES Trust

Project Report

Title and code:		**LA 01 - Preserving records and managing their life-cycle in a multi-provenance digital government environment – a case study on a government electronic system: SIGEPE**
Document type:		Final report
Status:		Final (public)
Version:		1.4
Research domain:		Control
Date submitted:		20/04/2017
Last reviewed:		17/04/2017
Author:		InterPARES Trust Project
Writer(s):		Claudia Lacombe Rocha, Flavia Cristina Diogo Claudino, Alexandre Gonçalves, Dayo de Araújo Silva Corbo, Fernando Matias da Costa
Research team:		Latin America TEAM

Document Control

Version history			
Version	Date	By	Notes
1.1	Apr. 27, 2015	Claudia	
1.2	May 12, 2015	Claudia; Alexandre; Dayo; Fernando; Flávia	Revision; annexes 1 and 2 attached
1.3	Jun. 18, 2015	Alexandre; Flávia; Fernando	Answers to research questions.
1.4	Jul. 16, 2015	Alexandre; Flávia; Fernando	Revision of questions and new information on data collection.
1.4 English v.	Nov. 17, 2015	José Márcio Rangel	Translation
1.5	Apr. 17, 2017	Claudia	Revision; layout editing

Table of Contents

Abstract 4
Research team 5
Background 5
Research questions 6
Goals 8
Methodology 8
Glossary of terms 8
Description of data collected 9
Findings 14
Conclusions 18
Products 19
References 21
Appendix 1 – Case Study Contextual Analysis Template 24
Appendix 2 – Questions to be answered by researchers on data collection 30

Abstract

This case study addresses the documents created and kept in the “Sistema de Gestão de Pessoas do Governo Federal – SIGEPE” (in English: Federal Government System for Personnel Management), which supports human resources activities within Brazil's Federal Executive Branch, by means of registering such activities and creating documents. SIGEPE is currently in development and implementation, and it expects to support 20 functions and 49 high-level business processes, of which have already been detailed and modeled 249 business processes. This study focuses on the module of the system that manages payroll-linked debts, more specifically the registration of the payroll-linked payees.

Government institutions have access to the system on the Internet, and the documents are kept in a centralized database and repository, under the responsibility of the SERPRO-DATAPREV consortium. Taking into account the term “private cloud” - defined in the InterPARES Trust Glossary as “ a deployment model in which a provider manages and supports infrastructure, platform, or software as a service for the exclusive use of a consumer” - and that such exclusive consumer is, in that case, the whole group of institutions under the Federal Public Administration, the conclusion was that SIGEPE is hosted in a “government private cloud.”

This report presents a brief presentation of the collected data on the records' characteristics and context of creation; the analysis of the scenario detected; and the recommendations to improve the system. Research questions are also answered considering all the analysis developed.

Preserving records and managing their life-cycle in a multi-provenance digital government environment – a case study on a government electronic system: SIGEPE

Research team

Lead Researcher(s): Claudia Lacombe Rocha
Project Researchers: Alexandre Gonçalves, Carlos Augusto Ditadi, Dayo de Araújo Silva Corbo, Fernando Matias da Costa, Flavia Cristina Diogo Claudino.

Background

Regarding the public administration in Brazil, records management activities began to take shape in the last two decades of the twentieth century. Although records management practice is not yet widely adopted, much has already been achieved in this field. The Records Management unit at the National Archives (Coordenação-Geral de Gestão de Documentos – COGED) has been working with federal government agencies advising on what relates to the implementation of records management procedures, the development of records management tools (classification plan & retention and disposition schedule) and the control of final disposition of records created by these agencies. Currently there is a set of norms that regulate the activities of records management on government which guides and supports the professionals working in the area.

In Brazil, records management is legally supported since the publication of the "Archives Law" (law 8159, January 8th, 1991) which explains the concept of record management and the decree n. 4173 (January 3rd 2002) which regulates the records management in the federal public administration. After this framework the National Council on Archives has published some directives which regulates the adoption of records management tools in public administration, the transfer of records to the archival institutions as well as the destruction of records, among others.

The decree 4073 already mandated the adoption by federal agencies of standards classification plan as well as retention and disposition schedule regarding administrative activities, which are common to all agencies. Since then these tools were adopted by the agencies and has been guiding the disposition of their records. The activities comprised in the classification plan are organized under the class "000 – general administration" and include the following subjects:

010 – organization and operation

020 – personnel

030 – supplies and equipment

040 – patrimony

050 – budget and finance

060 – documentation and information

070 – communications

080 - military personnel

090 – other matters relating to general administration

According to the regulations in force, the destruction of public records on federal government must be approved by the National Archives, after analysis of an “elimination list”, publication of an elimination science notice in the official gazette and the registration on “elimination term” to be maintained by the creator.

The transfer of records to the National Archives was regulated since 1997 by means of a specific norm, which was revised and updated, including procedures for digital records, by means of “Portaria Arquivo Nacional n. 252 (December 30th , 2015).

Many agencies are already following the records management procedures defined in the current legislation. Insofar as the personnel activities are now supported by the federal government personnel management system – SIGEPE – managed by the Ministry of Planning, and that this system does not allow creators to control these records, the agencies have lost the competence to manage their personnel records.

Research questions

SIGEPE's scenarios lead to some issues pointed out in the case study proposal which concerns the life cycle management and the preservation of the records created and maintained in the system:

1. Q: Are the digital entities created and kept in the system records?
   A: For the purpose of this case study, yes, as they record actions taken by the payroll-linked payees. They are digital records, once they have fixed documentary form (they are kept in PDF format), stable content (the system does not allow them to be overwritten or deleted) and the archival bond with other records that register the same action (all the records that take part in the registration of a payroll loan company are retrieved together), i.e., those records are related to one another as a set of records of the same activity. We must note that those records are currently duplicated (in SIGEPE and in SEI), though an authoritative copy is maintained in SIGEPE, where the most complete set of records is.
2. Q: Is the records' authenticity maintained?
   A: The authenticity is maintained by means of digital signature and/or system security controls. Some of the records carry a digital signature but many don't. The system, through its access control features, does not allow alterations in records after they are created. While records are kept in SIGEPE, they rely on the guarantees of a strong security system. However, when exported to SEI, there is no way to ensure authenticity, due to the lack of a digital signature during the exportation process. We suggest a digital signature provided by the system, instead of a personal one, at the time of exportation, as an authenticator of the records exported from SIGEPE.
3. Q: Who are the records' creators?
   A: The records studied here are created exclusively by the Ministry of Planning, Budget, and Management – MP, the government organization in charge of the registration of payroll-linked loan companies.
4. Q: Are the records maintained for as long as necessary?

A: We currently do not know if they are kept for as long as needed because, unlike what is established by the law in force, there is no retention schedule predefined by records management tools (classification scheme and disposition schedule that target the records concerning the core activities of the Ministry of Planning), which are still under construction. We have been informed that all records created and kept in SIGEPE will be maintained for 20 years, starting from their creation. Nevertheless, without such technical tools, we do not know which of those records are of permanent value, or should be maintained for more than 20 years. Furthermore, other records may need to be kept in the system for a shorter period. To sum up with, finishing up those records management tools is crucial to help keep records in the system for as long as necessary.

5. Q: Do creators have control over their records throughout their life cycle?
   A: Nowadays, the creator (the Ministry of Planning, Budget, and Management) generates two sets of records in different contexts: while in SEI there is control over the life cycle of the records in the digital dossier, in SIGEPE there is no such control. However, the records kept in SIGEPE are more complete instantiations, and should be regarded as the authoritative instantiations. As a solution, we suggest that all records created in SIGEPE be exported to SEI, and that the creator define the records kept in SEI as the authoritative instantiation of the set that records the registration of the payroll loan companies, and the set of records kept in SIGEPE would become just a copy.
6. Q: How is made the retention and disposition of records?
   A: At the moment, all records created in SIGEPE follow the same disposition rule: disposal after 20 years of retention. SERPRO, the service provider, is currently in charge of monitoring that in the system. Notwithstanding, it is strongly advised that the creators should be in charge of controlling disposition. We must stress that, in the case of the subject of this case study – the registration of payroll-linked payees –, there is not even a management tool to properly guide the records' final disposition, due to the absence of a classification scheme or a disposition schedule aimed at the MP's core activities.
7. Q: Who is in charge of records' retention and disposition? How is that done?
   A: The creator (MP) should be in charge of the disposition of records, although SERPRO currently carries it out, as the system does not offer creators the possibility of performing that activity by themselves.
8. Q: Who will have the final custody of the inactive records?
   A: According to Brazil's legislation on archives, the National Archives will hold that custody, and for that purpose a digital repository is currently being developed to be able to keep records with permanent value created by the entire federal government administration. We must also stress that SIGEPE does not yet offer the possibility of exporting records with permanent value to the National Archives' repository.

Goals

Issues being addressed

1. Definition of preservation strategies for the records created and maintained in the electronic system.
2. Identify controls required by the electronic system to manage records by each creator, including retention and disposition procedures.
3. Definition of responsibilities for the custody of the records kept within the electronic system on each life-cycle phase.

Objectives

Develop recommendations for the life cycle management of active and semi active records from different creators maintained in the same system.

Methodology

1. **Identify the case study target -** Define the body of potential records created in the electronic system for which a preservation plan has to be defined and which can be used as a pilot study relating the provenance control. This choice was made together with those responsible for the system, considering the modules already in use.
2. **Data collection** – Data about the context and maintenance procedures were collected through interviews, documentation analysis and diplomatics. Data collection was based on a template for contextual analysis and a set of questions to be answered by researchers (appendix 1 and 2). These templates were based on similar ones used for InterPARES 3 Project case studies.
3. **Management plan definition –** reflexion and analysis of data collected and proposal of a plan that includes strategies and protocol concerning the management of records life cycle by creator, considering control over retention and disposition and commitments responsibilities for the custody of records.
4. **Preservation plan definition –** reflexion and analysis of data collected and definition of a preservation plan that covers also the more suitable form of the record to be preserved (manifested or stored).
5. **Analysis and findings –** reflexion on issues faced and the plans addressed in order to enable the development of recommendations for similar situations.

Glossary of terms

Payroll-linked payee: companies authorized to provide services that are deducted automatically from the client's paychecks.

Payroll-linked deduction: authorization to deduct a certain amount from an employee's monthly paycheck, upon a service that is provided.

Cloud computing: a model for enabling ubiquitous, convenient, on-demand 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.

Cloud service: Functionality offered by a cloud provider that supports infrastructure, platform, software, or other services. A cloud service may be implemented using a public, private, hybrid, or community model.

Public cloud: A deployment model in which services (infrastructure, platform, or software) are managed by a third-party provider and made available to the general public.

Private cloud: A deployment model in which a provider manages and supports infrastructure, platform, or software as a service for the exclusive use of a consumer.

Private-owned government cloud: A deployment model in which a provider manages and supports infrastructure, platform, or software for the exclusive use of government agencies.

Description of data collected

SIGEPE is under development by the SERPRO[1]-DATAPREV[2] consortium, comprised of two large ICT companies of the federal government, by means of a contract held with the Secretariat of Public Management, of Brazil's Ministry of Planning, Budget and Management – MP.

The new system replaced the former human resource management system, called SIAPE, operating from 1989 to 2014 within the Federal Public Administration. Initially, SIAPE was aimed to centralize payroll processing, based on updating information provided by the government units that underwent staff payment in a decentralized way, which resulted in payroll calculations afterward. With time, all government foundations and organizations, either autarchic or state-controlled, maintained by the Federal Executive Branch and relying on the country's Treasury for their staff budget had to join SIAPE.

In 2014, SIAPE processed a payroll comprised of approximately 1,350,000 (one million, three hundered and fifty thousand) public servants (employees, retirees, pensioners and political pensioners) of 214 public organizations, adding up to 1,102 payment units all over the country.

The MP chose to replace SIAPE for a new system aimed at innovating and modernizing human resource management at organizations of the Federal Public Administration's civilian personnel system. The project, scheduled to take five years starting in 2012, is comprised of approximately 50 sub-projects. The system's modules are strongly

[1] The Federal Data Processing Service (SERPRO), founded in 1964, is a state-owned company mainatined by Brazil's Ministry of Finance. As a provider of Information and Communications Technologies services to the public sector, it is considered one of the largest ICT companies in the world.

[2] The Social Security Technology and Information Company (DATAPREV), founded in 1974, is maintained by Brazil's Ministry of Social Security. It was created from data processsing centers at social security institutions of the 1970s. Its main consumer is the National Social Securrity Institute, but it also provides services to the country's Internal Revenue Service and the ministries of Social Security, Labor and Employment, and Social Development and Fight against Hunger, among others.

dependent on each other, and share its infrastructure. Apart from SIAPE's already existing processes, several other processes concerning human resource management activities will be added and, as a result, almost all records to be created by the federal government organizations in the course of such activities will be created and kept in SIGEPE.

The SIGEPE Project joined another major project of the MP, kicked off in 2011, addressing the digitization of personnel file folders, which was named "Assentamento Funcional Digital – AFD" ("digital personnel files," in a free translation into English).

SIGEPE currently undergoes a process-oriented development, automating with the aid of computers the phases of a workflow, from the presentation of a certain plea (such as a benefit) to the fulfillment of the plea. A range of stakeholders create records along the phases of that workflow, putting together a history of the entire decision process.

In the beginning of 2014, SIGEP's portal got launched on the Web, offering the services already supported by SIAPE as well as some additional modules.

This case study approaches one of SIGEPE's sub-projects, called "Cadastramento de Consignatárias" ("registry of payroll-linked payees"), one of the first new modules implemented and launched in February 2014.

Service provider

The SERPRO-DATAPREV consortium is the provider of SIGEPE's services, as it is in charge of developing and hosting the system.

The MP hired the consortium to develop the system for the amount of R$ 97,320,530.60[3], not including system hosting or user help desk services, which are expected to be the object of another MP contract.

About 160 specialists are involved in the system's development, and distributed in teams located in several Brazilian cities, coordinated from SERPRO's headquarters in Brasilia, the country's capital.

Service users

In general, the service's users are all the organizations of the Federal Public Administration's civilian personnel system. Most of them are located in Brasilia, but there are units spread all over the country.

In the specific case of the SIGEPE module that is the object of this study, the service user is the Department of Civilian Personnel and Cross-unit Careers Management at the MP's Secretariat of Public Management, once that unit alone is in charge of registering payroll-linked payees.

Records creator

Ministry of Planning, Budget and Management – Secretariat of Public Management – Department of Civilian Personnel and Cross-unit Careers Management.

[3] Approximately 25 Million US dolars as of December 2015.

It is necessary to point out that, in general, the various federal government organizations within the civilian personnel system are all creators of records in most of SIGEPE's modules.

Activities that result in records' creation

The SIGEPE module that addresses the management of payroll-linked payees supports the registry of those companies, the investigation of irregular activities and processing the discounts on the payroll. This case study focuses exclusively on the registration of companies, including: receiving the proposing company's documents, validating such documents and all the other procedures up to the signature of an agreement.

Records created

A digital dossier is opened for the registration of each payroll-linked payee, which may gather the following documents:

1. pre-registration form;
2. documents required for registration approval;
3. work schedule;
4. agreement;
5. agreement excerpt;
6. notification;
7. notification of return;
8. official letter of return;
9. official letter to end the agreement;
10. term of agreement; and
11. addendum to agreement.

The norms addressing the registration of companies in order to operate payroll discounts establishes that the pre-registration form and all the other required documents must be sent, in paper form, to the MP's protocol and registry department.

The documents presented by the proposing company are analyzed so as to check whether they comply with all requirements, and then digitized and captured to SIGEPE's module for payroll-linked deduction. Each record is registered and identified individually in the system.

A dossier comprised of all those records is opened and registered at the MP's registry system. Paper dossiers would be opened until February 2015; since March 2nd all dossiers have started to be opened on the MP's electronic process system (called SEI – “Electronic Information System”), after documents were digitized. Electronic forms may be sent straight to the system, when the digital dossier has already been registered and given a registry number.

All the other records are created in the system, once the user inserts data in it. Those records are digitally signed, and the validation may be handled by means of login and password verification or of a digital signature granted by ICP-Brasil[4]. Furthermore, the records are exported and included in the digital dossier created in SEI for the registration of each company.

In SIGEPE, records can be altered during the registration process, i.e. they can be replaced by new, updated records. There is no version history control. Once the process is finished, the records created by the system can no longer be altered.

After the publication of an excerpt of the agreement, also generated by SIGEPE, on the federal government's official journal "Diário Oficial da União," the dossier is archived at the MP. From that moment on, the only record to be attached to the dossier is the official letter ending the agreement. After that, access to the dossier is given only to control organizations; additional records created in SIGEPE (addendum to an agreement and any record of changes in a company's data) stay solely in the system.

Maintaining records created in the system

Records concerning activities related to the registration of payroll-linked payees are duplicated: in the system and in the dossier (whether paper or digital) maintained by the MP.

Here follows the status of the records maintained in the system:

- Records are maintained in their manifested form, PDF format;
- Online storage in an exclusive repository of the module for payroll-linked deduction, where records are organized in a directory tree according to their date of creation ("sorting is made by means of a directory tree based on year/ month/ day");
- One main repository for all SIGEPE modules is expected to be launched;
- Digitally-signed certificates;
- Metadata stored in a data base. Users do not insert any metadata, while the following information is registered: identifier, name, path, and deletion indicator (deletion is logical only in the database, once the record is kept in the repository). Other metadata is expected to be stored in a document management system currently under development digital signature (date and time, author's name, signature file), date and time of creation, author.
- According to the SIGEPE team, "reliability is granted by means of hiring a public service provider (SERPRO and DATAPREV) that ensures data protection entirely. (…) Authenticity is guaranteed by the digital signature of those in charge of the records. (…) As for usability, the module for payroll-linked deduction does not offer a specific action. However, when it comes to the SIGEPE project as a whole, usability patterns have been defined to allow viewing and handling records. Such patterns will be incorporated in the module for payroll-linked deduction in the future."

In terms of security, as interviewees have informed, the following measures will be taken

[4] Brazil's official public key infrastructure.

in order to support the authenticity and preservation of records:

- Granting login/ password (for public servants, only for viewing purposes) and digital certification (for operators and managers) to control user access;
- Digitally signing all records created in the system;
- Ensuring a robust infrastructure by means of an agreement with a public provider company: the SERPRO-DATAPREV consortium.

Responsibility for records management

Paper dossiers (up to February 2015) would be archived at the main registry department of the Ministry of Planning, and managed within the Ministry's records management program, which is still being implemented. Digital dossiers (from March 2015 on) have been maintained in the MP's electronic process system, SEI[5].

The MP has started the design of a classification scheme and a disposition schedule, however the process was halted in its making due to internal issues.

Documents created in SIGEPE are stored and maintained in the system, though the MP has no management control over them. It is unclear for the MP that they are records, and that they ought to be managed as such.

Within the scope of SIGEPE, it has been debated whether the documents created in the system should be maintained exclusively in it, or if they should instead be captured by each organization's own records management system, as SEI is being implemented in several units of the Federal public Administration. That decision must be taken for each SIGEPE module, and it may vary, depending on the activity. The Secretariat of Public Management, the Department of Documentation and Information, and the Secretariat of Logistics and Information Technology of the Ministry of Planning, Budget and Management should participate in that debate along with the National Archives.

Disposition

At the MP, (paper and digital) dossiers are classified and disposed by the records management unit.

Most activities undergoing automation through SIGEPE are non-core business activities shared with all federal government organizations, and the records created along such activities are disposed according to a unified schedule in use by the entire Federal Pubic Administration[6]. The registration of payroll-linked payees is a specific activity of the MP; as such, the classification and disposition of records resulting from that activity shall be

[5] The “Sistema Eletrônico de Informações – SEI” (“Electronic Information System”) is an electronic process management system developed by Brazil's federal court of the 4th region (TRF4) that was drafted as a software solution for the government's National Electronic Process project. The use of SEI is not mandatory among organizations of the Federal Public Administration, although the Ministry of Planning, Budget, and Management strongly recommends it.

[6] “The classification and disposition of records concerning non-core activities of the Public Administration,” an instrument approved by means of the Resolution no. 14 of the National Council on Archives, of October 24th 2001, and made mandatory for the Federal Public Administration by means of the Decree no. 4,043, of January 3rd 2002.

approached in the classification scheme and disposition schedule for the Ministry's core business activities, still in development.

According to SIGEPE's team: digital records created in the system shall be managed by the system:

> "(...) [records are] not yet under SIGEPE's management. Nevertheless how that management will take place is already being discussed (…) deletion management is not operational yet, and all documents are being kept in the outsourced infrastructure (public provider)."

Responsibility for records preservation

The Ministry of Planning is responsible for the preservation of digital dossiers, while SIGEPE's team is in charge for that of the records maintained in the system.

SIGEPE's team understands that there should be concern over records preservation, but the only step taken towards it, as they mentioned, was the choice for the PDF/A file format, followed by the possibility that, in the future, documents are created in the HTML5 format.

Findings

The analysis of the information collected draws attention to some aspects of the characteristics of the records created, of the procedures aimed at their maintenance and preservation, and of the control over their life cycle, which are pointed as following.

Identification of the records created and maintained in SIGEPE

It was verified that the registration of payroll-linked payees results in the creation of two sets of digital records comprised of the same records:

> **a-** the digital dossier kept in SEI (digitized copies of the documents presented by the candidate to payroll loan company + records created by SIGEPE along the registration process and exported to the digital dossier; after the agreement is signed, the official letter to end the agreement is attached to it).
>
> **b**- records concerning the registration of each payroll-linked payee kept in SIGEPE (digitized copies of the documents presented by the candidate to payroll loan company + records created by SIGEPE along the registration process).

According to the SIGEPE team, the records in the digital dossiers are the original records of the action of registering payroll-linked payee, and the ones kept in SIGEPE are regarded as copies of those records.

It is necessary to recall the concept of record, defined as "a document made or received in the course of a practical activity as an instrument or a by-product of such activity, and set aside for action or reference." Thus, **if** the actions that take place following the registration of payroll loan companies refer exclusively to records in the digital dossiers kept in SEI, it is possible to present this consideration. However, if the actors involved in the process refer to records kept in SIGEPE, these ones must also be regarded as original records.

On the other hand, we recall the concept of “authoritative copy,” defined in the InterPARES 3 Glossary as “the instantiation of a record that is considered by the creator to be its official record and is usually subject to procedural controls that are not required for other instantiations.” Then the MP would be able to classify the digital dossier kept in SEI as an “authoritative copy” of the set of records documenting the registration of payroll-linked payee. Consequently the digital dossier would be included in the MP's archival holdings, complying with disposition controls established in specific instruments, and the set of records kept in SIGEPE would just be other copies, not necessarily subject to strict records management controls.

In that case, we must draw attention to certain issues: (1) the set of records concerning the registration of payroll-linked payee kept in SIGEPE maintains records that are not in the dossier kept in SEI, which must not occur; and (2) the source of reliable information to be referred to in future actions should be the digital dossier kept in SEI.

So as to allow the MP to make that decision, another aspect to be taken into consideration is related to the procedures currently in operation in SIGEPE in terms of creating and exporting records, once the records kept in the system carry digital signatures, while the ones exported to SEI do not keep that signature associated. The professionals in charge of SIGEPE concluded that procedure will have to change, so that the records can be exported together with their digital signatures and be taken as original records.

Use of digital signature

In SIGEPE, digital signature with digital certification is used in order to authenticate records created in the system, as well as to authenticate user access to the system.

The use of digital signature to authenticate records created in the system seems to be a convenient procedure, as those records will be exported to SEI. Notwithstanding, we must underline the fact that digital signature presents drawbacks in the long term when it comes to its capacity to state the authenticity of a record because, in case we need to convert a digital record as to preserve it, the new file, resulting from that conversion, will no longer bear the signature. In that case, metadata must register the information that the record has been received with such signature (signature code, signer's public key, signer's identification, signature properties) and that it has been verified (validation date and result of validation).

The authentication of user access to the system can be held in two ways: by means of login and password verification, in the case of public servants in general wishing to make queries, or by means of digital certification issued by a certification authority of ICP-Brasil, in the case of managers and operators that carry out personnel management activities, authorize actions, and create records. That type of use can be considered appropriate, as it provides more security for the authentication of users designed to perform procedures demanding a higher level of control. Furthermore, the spectrum of users that require digital certification is limited, which does not imply major increase in costs.

Metadata

The records' metadata currently registered by SIGEPE comes down to only: identifier, name, path and deletion indicator.

Metadata is an important element to support the authenticity, management and preservation of records. Therefore we suggest a broader metadata set including, in the minimum, the identity and integrity metadata recommended by the InterPARES Project, according to its, "Benchmark Requirements for Supporting the Presumption of Authenticity of Electronic Records." Another reference to follow are the records' metadata listed in the "Requirement Model for Digital Records Management Systems" ("Modelo de Requisitos para sistemas informatizados de gestão arquivística de documentos", in Portuguese), a.k.a. "e-ARQ Brasil".

Storage of records

The storage of records is currently carried out in a directory structure organized by date of creation (year/month/day), which does not help retrieve the archival bond between records, as recommended in laws and best practices in use for records. We must stress that the archival bond is the relationship that links each record to the other records that participate in the same activity, a core feature of records that distinguishes them from other types of documents, and yet a strong element of support to their authenticity.

We must also refer, in the same field, to the "Guidelines for the Implementation of Trustworthy Digital Repositories for Records" ("Diretrizes para implementação de repositórios digitais confiáveis de documentos arquivísticos," in Portuguese), approved by Brazil's National Council on Archives in its Resolution no. 39 (Apr. 29, 2014), as well as to InterPARES Project's booklet "Creator Guidelines – Making and Maintaining Digital Materials: Guidelines for Individuals." The National Council's guidelines for records repositories state that "a digital repository of records must be able to organize and retrieve records, so as to maintain their archival bond." The InterPARES Project's guidelines recommend that digital records should be gathered in a logical manner, so that "all records related to the same activity or subject, or of the same type, can be easily identified and retrieved as part of one conceptual grouping, as needed."

In the case of the registration of payroll-linked payee, all the records related to the same registration action have an archival bond. Thus, according to such guidelines, those sets of records ought to kept so that the archival bond can be easily retrieved. The organization of the directories by date does no good to the retrieval of records, while the proposal based on gathering sets of records of the same registration action may facilitate the retrieval of their archival bond. Nevertheless, grouping records in directories is not indispensable, once registering identity metadata allows records to be grouped whenever necessary.

Responsibility for the management of records created in SIGEPE

Considering this case study's target, i.e. the records created along the process of registration of payroll-linked payee, we found out that the MP holds responsibility over the management of (paper and digital) dossiers that gather records of each registration action. As for the records kept in SIGEPE, the Ministry has no control over them.

The SIGEPE team suggests changing features of the system so that: (1) the records exported by SIGEPE and kept in dossiers in SEI can be regarded as "authoritative copies", and (2) the records kept in SIGEPE can be considered as copies of them that do not require any management control. In that case, according to what was suggested, the responsibility for the management and disposition of the records kept in SIGEPE would be of those in charge of the system.

That proposal would facilitate disposition procedures targeting the records kept in SIGEPE, as they could be eliminated without the need to comply with any strict control from Brazil's archival legislation, due to the fact that the "authoritative copies" (in the dossiers) would be disposed appropriately by the MP.

We must note that SIGEPE's maintenance team has the physical custody of the records kept in the system, while the organization that created the records holds the legal custody, i.e. the legal responsibility for the records aggregation (preservation, access and disposition). Therefore, the disposition of records kept in SIGEPE, even if they are not seen as "authoritative copies," must be planned and monitored by the MP's records management unit. It is important to note that it is not clear to the actors involved (SIGEPE's team or the MP) that the creator has the legal custody of the records, which needs to be elucidated.

Additionally, that view may not comprehend all records created in the other modules of the system. According to what was reported in the section "Identification of the records created and maintained in SIGEPE," we must identify in each module what records are created and if there are instantiations of them outside the system; for each case, the responsibility for the management and disposition of the records must be determined. It is very much likely that there will be original records that only exist in SIGEPE, and the system will need to provide support to creators aiming at the disposition of those records.

The disposition of records is the creator's responsibility. Besides, clearly defining the records' provenance at the moment of their transfer to the historical archives is an essential step of archival processing, once it is also an important element to determine the context of a group of records, which supports their authenticity. According to Adrian Cunningham, "(…) the thing that separates archives from other forms of information is that they derive their meaning and value from their provenance. If you do not know the provenance of a document, then the document can be no more than a source of information out of context – an information object that is largely devoid of wider meaning." (Cunningham, 2007)

Finally, we reinforce that the custody of the "authoritative copies" belongs to the records' creator and, considering that there are several creators in most of SIGEPE's modules (organizations of the Federal Public Administration that use the system), SIGEPE needs to allow each creator to carry out the disposition of the records that form their archives.

Preservation and security of records created in SIGEPE

Data collection showed that the team in charge of SIGEPE holds the responsibility for the preservation of the records created and maintained in the system. That may be appropriate, as the team clearly have the physical custody of the records, but the MP's records management unit must watch how the job will be handled.

The records are maintained in its manifested form, in PDF format, and it is expected that they will be created in HTML5 in the near future. Those choices are seen as appropriate for long-term preservation, for records with long life expectation. We suggest monitoring those formats and converting them in the future, in case they become obsolete.

The use of digital signature in records may present problems in the long term, which leads to the need of certain measures, as mentioned in the section that addresses digital signature.

A robust infrastructure for hosting the system is provided by the SERPRO-DATAPREV consortium (comprised of two companies with large operations in the IT sector, as described in the section “Description of records and the context of their creation”), which ensures appropriate access control and records' integrity. Besides, as government-owned companies, they offer a high level of trustworthiness in terms of permanence of the services provided and of control over access to information.

Despite some concerns over records' preservation, there is no digital preservation policy. The formalization of a policy of that kind would be important, and so would be defining medium- and long-term strategies.

Conclusions

The findings of the case study confirmed that the creators do not have control over the life cycle of their records related to the activities supported by the SIGEPE electronic system. The pilot chosen for the case study – management of payroll-linked debts – refers to an activity exclusive of the Ministry of Planning, what is an exception on the context of SIGEPE system, once the majority of the system modules supports activities that are performed by all the federal government agencies. Even considering only the focus of the case study, it was clear that the records were created and maintained within the system and that the creator didn't have any responsibility for its maintenance nor the possibility of controlling the disposition of its records according to the rules in force. This situation appears to be more complicated when facing the other system modules, that are used by various creator and maintain records of multiple provenance.

It was noticed that those responsible for the system development were not aware that the system created archival records and that those records should be part of the archival collections of each of the government agencies using the system. Moreover, these people were not aware that the disposition of the records should be conducted respectively by their creators. At first, that is why they didn't designed features in the system to support the records management appropriately.

Conducting the case study and having all the debates (between the research team and the system developers) that emerged during the research, was very productive and made it possible to highlight the need for implementing records management and enabling the control of records by its creators. Accordingly, some approaches to enable creators to have control over their records were raised. Initially was considered the possibility of developing specific records management module in the SIGEPE system. However, in the end, the system developers come to the conclusion that this solution would be very complex. Thus, it was decided that the ideal would be to export the records created in the system so that each creator could keep them in their own records management system.

This decision points out the complexity of performing the records management of records from multiple creators on a shared system.

Even being a service provided by a government private cloud, in which there seems to be no commercial interests, maintenance and preservation of archival records does not seem to be a priority. At the end of the case study, those responsible for the system development seemed aware of the need to improve the system. Nevertheless, two years after concluding the study, nothing has been done to implement the recommendations. It seems that the priority of this system, as many similar others, is only the immediate moment of performing the activity.

Products

After analyzing the data collected and discussing with those responsible for the development of the system some possibilities to deal with the issues found, some recommendations were drawn up:

1. Need to expand the list of metadata of the records created within the system so as to include identity and integrity metadata. It is recommended to include, in the minimum, the identity and integrity metadata recommended by the InterPARES Project, according to its, “Benchmark Requirements for Supporting the Presumption of Authenticity of Electronic Records”.
2. Register digital signature metadata when the record is stored (signature code, signer's public key, signer's identification, signature properties) and when the signature is validated (validation date and result of validation). This metadata supports the verification of original digital signature in the future, when the file has been converted due to digital preservation.
3. Explicit the records' archival bond by registering information that retrieves that bond through metadata.
4. In the case of the module for payroll-linked deduction, in order to consider the dossier in SEI as the authoritative copy, ALL records created in SIGEPE concerning a payroll loan company must unarguably be inserted in the dossier kept in SEI.
5. Expand the analysis performed in the system module chosen for the case study for all the other modules. So that it is possible to identify, in each SIGEPE module, the records created in the course of activities supported by the system, and how the management of records will be carried out – as well as the control over their life cycle, considering the following steps:
   - identify records created in the SIGEPE module in question;
   - identify if (all of) those records exist simultaneously outside the system;
   - [if yes] identify which is the “authoritative copy” of the records;
   - define the responsibility for the custody of the records identified (inside and outside the system);
   - clearly define the responsibility for the management of the records created.

Note: That identification must be implemented by the team in charge of SIGEPE, accompanied and supported by the National Archives and by the MP's Records Management unit.

6. Carry out procedures that enable control over the life cycle of records created and maintained in the system, especially disposition (disposal or transfer):
   - in the case of the "authoritative copies" of the records kept in SIGEPE, actions to help records creators accomplish the appropriate final disposition must be implemented, according to the law in force;
   - In the case of the records kept in SIGEPE that were not appraised as "authoritative copies," the MP's Records Management unit must monitor the disposal of such copies.
7. Formally define a digital preservation policy aimed at records created and maintained in SIGEPE.

References

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **e-ARQ Brasil – Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos**. Rio de Janeiro: 2011.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Classificação, temporalidade e destinação de documentos de arquivo relativos às atividades-meio da administração pública.** Rio de Janeiro: Arquivo Nacional, 2001.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 2, de 18 de outubro de 1995. Dispõe sobre as medidas a serem observadas na transferência ou no recolhimento de acervos documentais para instituições arquivísticas públicas. **Diário Oficial da União**, Brasília, DF, 24 de outubro de 1995. Disponível em: <http://conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?from%5Finfo%5Findex=41&infoid=53&sid=46>. Acesso em 08 de maio de 2015.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 5, de 30 de setembro de 1996. Dispõe sobre a publicação de editais para Eliminação de Documentos nos Diários Oficiais da União, Distrito Federal, Estados e Municípios. **Diário Oficial da União**, Brasília, DF, 11 de outubro de 1996. Disponível em: <http://conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?from%5Finfo%5Findex=31&infoid=56&sid=46>. Acesso em 08 de maio de 2015.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 14, de 24 de outubro de 2001. Aprova a versão revisada e ampliada da Resolução nº 4, de 28 de março de 1996, que dispõe sobre o Código de Classificação de Documentos de Arquivo para a Administração Pública: Atividades-Meio, a ser adotado como modelo para os arquivos correntes dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR), e os prazos de guarda e a destinação de documentos estabelecidos na Tabela Básica de Temporalidade e Destinação de Documentos de Arquivo Relativos as Atividades-Meio da Administração Pública. **Diário Oficial da União**, Brasília, DF, 8 de fevereiro de 2002. Disponível em: <http://conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?from%5Finfo%5Findex=21&infoid=65&sid=46>. Acesso em 08 de maio de 2015.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 24, de 3 de agosto de 2006. Estabelece diretrizes para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas públicas. **Diário Oficial da União**, Brasília, DF, 7 de agosto de 2006. Disponível em: <http://conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?from%5Finfo%5Findex=11&infoid=75&sid=46>. Acesso em 08 de maio de 2015.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 25, de 27 de abril de 2007. Dispõe sobre a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR. **Diário Oficial da União**, Brasília, DF, 27 de abril de 2007. Disponível em:

<http://conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?from%5Finfo%5Findex=11&infoid=206&sid=46>. Acesso em 08 de maio de 2015.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 32, de 17 de maio de 2010. Dispõe sobre a inserção dos Metadados na Parte II do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil. **Diário Oficial da União**, Brasília, DF,18 de maio de 2010. Disponível em: <http://conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?from%5Finfo%5Findex=11&infoid=509&sid=46>. Acesso em 08 de maio de 2015.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 37, de 19 de dezembro de 2012. Aprova as Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais. **Diário Oficial da União**, Brasília, DF, 20 de dezembro de 2012. Disponível em: <http://conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?from%5Finfo%5Findex=1&infoid=832&sid=46>. Acesso em 08 de maio de 2015.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 39, de 29 de abril de 2014. Estabelece diretrizes para a implementação de repositórios digitais confiáveis para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas dos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR. **Diário Oficial da União**, Brasília, DF, 30 de abril de 2014. Disponível em: <http://conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?from%5Finfo%5Findex=1&infoid=947&sid=46>. Acesso em 08 de maio de 2015.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 40, de 9 de dezembro de 2014. Dispõe sobre os procedimentos para a eliminação de documentos no âmbito dos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR. **Diário Oficial da União**, Brasília, DF, 11 de dezembro de 2014. Disponível em: <http://conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?from%5Finfo%5Findex=1&infoid=1017&sid=46>. Acesso em 08 de maio de 2015.

CUNNINGHAM, Adrian. **O Poder da Proveniência na descrição arquivística, uma perspectiva sobre o desenvolvimento da segunda edição da ISAAR(CPF).** Rio de Janeiro: Arquivo Nacional. Revista Acervo, v. 20, p. 77-94, 2007.

INTERPARES PROJECT. Requirements for assessing and maintaining the authenticity of electronic records in: **The long term preservation of authentic electronic records: findings of the InterPARES Project**. Editor Luciana Duranti, 2005.

INTERPARES 2 PROJECT. **Diretrizes do produtor - a elaboração e a manutenção de materiais digitais**: diretrizes para indivíduos. Vancouver: InterPARES Project. School of Library, Archival and Information Studies - The University of British Columbia; 2007. Disponível em: <http://www.interpares.org/ip2/display_file.cfm?doc=ip2_creator_guidelines_booklet--portuguese.pdf>. Acesso em: 5 maio 2015.

INTERPARES 2 PROJECT. **Diretrizes do preservador – a preservação de documentos arquivísticos digitais:** diretrizes para organizações. Vancouver: InterPARES Project, School of Library, Archival and Information Studies, The University of British Columbia; 2007. Disponível em:

<http://www.interpares.org/ip2/display_file.cfm?doc=ip2_preserver_guidelines_booklet--portuguese.pdf> Acesso em: 5 maio 2015.

INTERPARES 2 PROJECT. **Policy Framework - A framework of principles for the development of policies, strategies and standards for the long-term preservation of digital records.** 2008. Disponível em : <http://www.interpares.org/ip2/display_file.cfm?doc=ip2%28pub%29policy_framework_document.pdf>. Acesso em: 5 maio 2015.

INTERPARES 3 PROJECT. **Base de dados de terminologia do InterPARES 3**. Disponível em: <http://www.interpares.org/ip3/ip3_terminology_db.cfm?letter=az>. Acesso em: 5 maio 2015.

Appendix 1 – Case Study Contextual Analysis Template

The purpose of this template is to enable the gathering of contextual information that provides knowledge on the contexts in which records are created (juridical-administrative, procedural, provenance, documentary and technological contexts).

In order to gather such information, the following procedures are recommended:

- *the researcher shall make previous effort so as to retrieve the information that is available to the public;*
- *the researcher shall gather the remaining information by means of interviews with representatives of the organizations involved;*
- *the researchers shall explain the reasons for lack of information, when applicable.*

This template applies to services provided on the Internet. Those services may be private, or provided by a government organization aiming to serve others.

I – TEST BED

This section has been structured in two subsections. The first concerns the organization that provides the Internet service. The second aims to describe the group of individuals or organizations that are potential users of the service provided; also, it may show whether those users comprise a homogenous group, or there are differences concerning the features approached.

I a – Service provider organization

Legal and normative framework of the service provider organization

Name

- *Official name and other names.*

Location

- *Country, state and/or city that exerts the most legal influence over the service provider.*

Origins

- *Information regarding how and why it began its activities, official founding date and/or founding event.*
- *A brief history of the organization.*

Legal Status

- *Legal status. For example: "federal government organization", "research group", "non-governmental organization" etc.*

- *Year of legal establishment, if applicable.*
- *Other relevant legislation concerning the service provider. For example: "copyright", "company regulations" etc.*

Norms

- *Information about any non-legally required standards, methodologies, codes or regulations from organizations, disciplines, traditions or professional associations that are subscribed to by the service provider.*

Governance framework of the service provider organization

Mandate and Philosophy

- *Information about the responsibilities of the service provider that were legally given to it.*

Mission

- *Formal statement of the mission: the stated way in which the organization is working towards the mandate.*

Administrative Framework

- *Structure, including organizational chart (if relevant).*
- *Information on how the service provider is managed. For example: co-operative, association, partnership.*

Functions

- *Major functions that the service provider undertakes. For example: administration, research, training.*
- *Statement of whether the service provided is the organization's main activity.*

Funding

- *Information about the sources of revenue related to case under study.*

Resources (physical)

- *Information about the physical context in which the service provider is working, including equipment and infrastructure.*

Human Resources

- *Employees, members and partners (number, areas of specialization, qualifications, turnover).*

<u>I b – Service user organization(s)</u>

Legal and normative framework of the service user

Name

- *Official name and other names*

Location

- *Country, state and/or city that exerts the most legal influence over the service user.*

Origins

- *A brief history of the organization.*

Legal Status

- *Legal status. For example: "federal government organization", "research group", "non-governmental organization" etc.*
- *Year of legal establishment, if applicable.*
- *Other relevant legislation concerning the service user. For example: "copyright", "company regulations" etc.*

Norms

- *Information about any non-legally required standards, methodologies, codes or regulations from organizations, disciplines, traditions or professional associations that are subscribed to by the service user. For example: archival methodology.*

Governance framework of the service user organization

Mandate and Philosophy

- *Information about the responsibilities of the service user that were legally given to it.*

Mission

- *Formal statement of the mission: the stated way in which the organization is working towards the mandate.*

Functions

- *Major functions that the service user undertakes. For example: administration, research, training.*

Funding

- *Information about the sources of revenue related to case under study.*

Resources (physical)

- *Information about the physical context in which the service user is working, including equipment and infrastructure.*

Human Resources

- *Employees, members and partners (number, areas of specialization, qualifications, turnover).*

II – RELEVANT ACTIVITIES AND RECORDS

This section aims to gather information about: records management practices, activities resulting in records/ documents, and the records themselves.

Activities resulting in the creation of the relevant records

- *General description of your organization's functions and/or list type of activities that result specifically in the creation of records*
- *Identify records creators.*

Records resulting from activities

- *Main records resulting from the activities listed above, and maintained by the service provider.*

Existence of a records management program

- *If they exist, describe the activities and any policy related to records management that the service provider and/or user might have.*

Individuals responsible for records maintenance

- *Identify the individuals(s) responsible for keeping the records after their creation. This might be among the personnel of the service provider or user organization.*

Existence of maintenance strategies

- *If they exist, identify the complex of practical means formally articulated or simply implemented for recordkeeping (service provider and user). This includes:*
  1. *The location in which the records are kept,*
  2. *The medium in which records are kept,*
  3. *A description of how records are organized,*
  4. *A brief description of any methods used in the records management,*
  5. *A brief description of any methods used to attempt to avoid technological obsolescence while the records are still active or semi-active.*

Legal Requirements and Constraints

- *Description of how the relevant laws influence the creation, form, content, identity, integrity, organization and maintenance of the records (for instance, the impact of the access to information act).*

Normative Requirements and Constraints

- *The written or unwritten rules of a specific discipline or area of thought related to the service provided. The written or unwritten rules may be related, but not limited to scientific, artistic and ethical requirements and constraints.*
- *Description of how these rules influence the creation, form, content, identity, integrity, organization and maintenance of the records (for instance, the rules that enforce the protection of the name of a person demanding information from a government organization).*

Technological Requirements and Constraints

- *Technological features related to the service provided by the test-bed, concerning the context of the study specifically.*
  1. *Hardware,*
  2. *Architecture (e.g., network topology, infrastructure, hardware),*
  3. *Creation or input tools (e.g., software, camera, microphone),*
  4. *Processing tools (e.g., software, console),*
  5. *Types of media created (e.g., graphic, textual, audio),*
  6. *Formats created (e.g., .pdf, .doc, .jpg) and identify any particular challenges related to their maintenance and preservation.*
- *Description of how these features influence the creation, form, content, identity, integrity, organization and maintenance of the records.*

Factors of satisfaction of the services provided

- *Description of the user's perception about the services rendered by the provider related to the following aspects:*
  1. *Tools for records creation, access, use and retrieval;*
  2. *Technical support service efficient and timely;*
  3. *Periodicity of presenting problems of service provided;*
  4. *Resolution capacity of problems in minimal time;*
  5. *Attention to requests for service improvement;*
  6. *Perception of service quality.*

III – AUTHENTICITY REQUIREMENTS OF THE DIGITAL RECORDS UNDER STUDY

This section aims to complement the information previously gathered, which are related to documentary and procedural contexts.

This information seeks to support the appraisal of authenticity (identity and integrity) of the records, by means of identifying the use/ existence of metadata and security and control mechanisms.

Check the existence of:

a- Identity Metadata:

- Names of persons involved in the creation of the record (author, writer, originator, addressee, recipient);
- Title/subject (action or matter);
- Documentary form (letter, report, etc.);
- Digital presentation (format, wrapper, encoding, etc.);
- Dates of creation and transmission;

- Expression of documentary context (e.g., classification code, folder or directory, etc.);
- Indication of attachments (if applicable);
- Indication of copyright or other intellectual rights (if applicable);
- Indication of the presence or removal of digital signatures;
- Indication of other forms of authentication (e.g., corroboration, attestation, etc.);
- Draft or version number (if applicable);
- Existence and location of duplicate materials outside of the system (indicate which is the authoritative copy).

b- Integrity Metadata:

- Name of the persons/office responsible for carrying out the action within the record;
- Name of office/person with primary responsibility for keeping the record (may be same as the one above);
- Indication of annotations;
- Indication of technical changes to either material or application;
- Access restrictions (if applicable);
- Access privileges (if applicable);
- Planned disposition.

c- Auditing and Tracking Metadata

d- Unauthorized Access Protection Devices

e- Security Devices

- Existence of backup copies
- Security and risk policies

f- Organization

- Organization of digital materials into logical groupings (classification scheme, identity metadata).

g- Authentication tools

- Use of authentication techniques that foster the long-term preservation of digital records (technology-independent vs. technology-dependent)

Appendix 2 – Questions to be answered by researchers on data collection

1. Which activities generate the digital records under study?
2. Which records are created in the system in the course of such activities?
3. Who is the creator of the records?
4. How are the records created? (inform about: internet technologies, web portal, etc)
5. In what formats are the records maintained (eg. Word or Excel files, PDF/A, html, txt, database etc)?
6. Is there a paper copy of those records?
7. Are these digital records linked by an archival bond to records on other media? If yes, what records? How is their relationships made explicit?
8. What are the key formal elements, attributes, and behavior (if any) of these digital records?
9. What metadata is manually added to the records by their author and their creator? What metadata is automatically generated and attached to the record?
10. What are the digital components of these digital records?
11. How are these digital records identified (e.g., is there a [persistent] unique identifier)?
12. Are there any concerns with the authenticity, reliability, usability and data protection of these records? How is authenticity, reliability, usability and data protection guaranteed?
13. Who (juridical person) is responsible for records maintenance? Are they under custody of the creator's archive?
14. Is there a classification schema and disposition rules applied to these records?
15. Who (juridical person) is responsible for records disposition?
16. Once the records are created, how are they maintained? (inform about: data base, repository, online/offline, type of midia, separated by agencies/all agencies mixed together)
17. How are changes to these digital records made and recorded?
18. Is there a risk plan established?
19. How is security assured?
20. Is there any concern with records preservation? Which procedures are in use?
21. Who is responsible for records preservation?