Towards Automatic Integration of Information Security Governance and Management using a BPMS approach

Angel J. Varela Vaca and Rafael M. Gasca
Universidad de Sevilla, Dpto. Lenguajes y Sistemas Informáticos,
Avda. Reina Mercedes S/N, 41012, Sevilla, España
Quivir Research Group, http://www.lsi.us.es/~quivir
{ajvarela, gasca}@us.es

Abstract- ***The information security management is more and more carried out by means of business processes although disregarding the quality of management enough. In order to improve that quality, we propose to carry out the automation of the information security governance. To achieve a high maturity level in the information security management, the integration of processes for good governance is needed, which enables to ensure the maturity level 4: Qualitatively Controlled, such as ISO/IEC 21827:2008 proposed. This level allows establishing measurable quality goals and objectively managing performance. This work enables to reach these levels by using business process management systems to implement a good information security governance, combined with the integration of business processes for the information security management.***

I. Introduction

Nowadays, Information has become in a corner stone in the information society. Information is a crucial asset to any business therefore it must be correctly protected. Currently, it is common to find organizations that offer and consume services and processes over the Internet. These services and processes consume a wide range of information (social network opinions, news feeds, financial data, etc.) that is probably used for decision-making processes. For this reason information assurance is an essential factor that has to be ensured in the IT systems for the organizations. Since, an information leakage can suppose terrible consequences [1] such as lack of reputation or privacy loss among others.

Organizations are using business processes as core for the business enterprise management. According to this idea, business processes are being created to the Information Security Management (ISM). In the majority of cases a Good Governance of the IS is left out instead of becoming to a strategic asset in the last years. For instance, Small and Medium Enterprises (SME) composed almost the 98 percent of the business landscape in Spain. Indeed, the 19.5 percent of Spanish enterprises are currently breaking security regulations like LOPD or LSSI [2] because of an incorrect way of directing Information Security Governance (ISG).

The Governance and Management of the IS in conjunction allows protecting the information provided by processes that comply with the security requirements related to the authenticity, integrity, confidentiality, availability and traceability.

The question is how to propose the automatic integration of both competencies with the idea to reach the level of maturity in the security management according to the business goals. This vision is being carried out for the ISG/ISM in the area of development of projects of R&D in the Research Group "Tecnologías Inteligentes y de Seguridad en Sistemas de Información" which belongs to Foundation for Investigation and Development of Information Technologies of Andalusia (FIDETIA) and has been certified in the standard ISO/IEC 27001:2013 [3] in the last years.

The rest of the paper is structured as follows: Section II show an overview of ISG by means of introducing the basis and the framework followed; Section III brings both automation and business processes up for a good ISG; Section IV shows a successfully case study where processes and mechanisms to automate ISG are shown in practice; in Section V conclusions are drawn and future work is proposed.

II. Information Security Governance

It is widely accepted that Information Security Governance (ISG) is a subset of corporate or enterprise governance. The IT Governance Institute (2001) defines enterprise governance as the "set of responsibilities and practices exercised by the board and executive management with the goal of **providing strategic direction, ensuring that objectives are achieved**, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly". Then by extending this definition, ISG could include: security responsibilities and processes, risk assessment and management, compliance with security policies, rules, regulations and legislation, monitoring and control of security activities. Our proposal is focused in the automation of ISG with computational tools.

The framework followed; such as shown in Fig. 1, implements three main processes:

- **Direct** where Security Governance can establish policies and define a pack of metrics to be measured in an interactive and step by step way.

- **Monitor** where measurements are gathered during the processes are enacted. Monitoring requires to include pieces of software at the processes (imperceptible for customers) that enable to collect information about the metrics.
- **Evaluation** which enables the Security Governance to analyse the different metrics in order to decide whether new countermeasures should be applied. This process can be carried out manually when governance needs or a report can be obtained regularly.

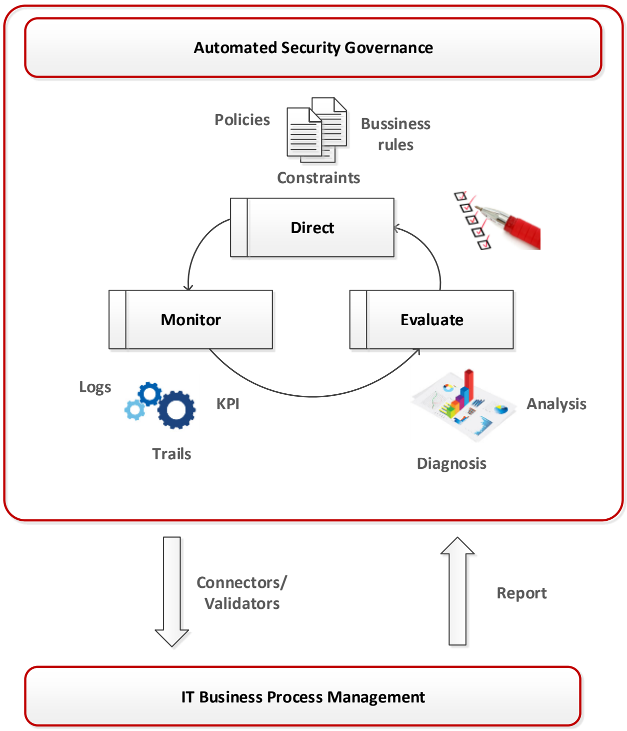


Figure 1. Security Governance framework

The most important international standards related to ISG have been established in the publications of S. H. von Solms and R. von Solms [3], the recent ISO/IEC 27014:2013 [5] and COBIT 5 for Security Information [6].

S.H. von Solms and Rossouw von Solms [7][8][9] have published a wide number of articles related to ISG, but from a theoretical point of view. In their book Information Security Governance [4], they established a specific description of ISG. Also, ISO/IEC 27014:2013 standard established that ISG is a “system by which an organization's information security activities are directed and controlled” and COBIT 5 provides a framework that helps enterprises in achieving their objectives for the governance and management of enterprise IT in a holistic manner. COBIT 5 for Information Security is integrated on the COBIT 5 framework. It focusses on information security and provides more detailed and more practical guidance for information security professionals and other interested parties at all levels of the enterprise.

But all this theory of these standards is necessary to put in practice furthermore integrating it within information security management.

III. AUTOMATIC INFORMATION SECURITY GOVERNANCE USING BPMS

To accomplish the objectives previously set for the ISG, we propose to automate those processes by means of Business Process Management Systems (BPMS). This kind of systems enables to align the processes of good ISG with the information security management (ISO 27001/2013) and also carry out the main tasks for the ISG: Direct, Evaluate and Monitor. In order to do that, we propose to integrate together the processes already established for the Information Security Management and the processes for ISG. Therefore the following items must be defined in those systems:

- The **organizational structure** which governs the information security in which information security management must be integrated.
- The **business processes of ISG** which has to be integrated with the management processes in such a way which enables to carry out the governance’s task from the task in the information security management.
- The **business rules** established by the direction that have to be included in the business processes of the IS Governance.

All of that enables to reach a level of maturity in the IS management within organization which rise up to maturity level 4 Qualitatively Controlled proposed by ISO 21827:2008, moreover it enables to establish measurable quality goals objectively managing performance of the IS.

Nowadays, Business Process Management (BPM) has become a cutting-edge field in IT arena. BPM [10] consists of a strategy to administrate and improve the operational aspects of businesses by means of a cycle encompassed by the following stages: modelling, enactment, and evaluation. It constitutes a methodology of good practices within a technological solution. Currently, Business Process Management Systems (BPMS) constitute a set of services and tools that make easy the management of business processes. Here, the management is considered as: analysis, definition, execution, simulation, monitoring, and control of processes. Furthermore, these systems enable the human interaction with processes by web forms providing mechanisms to enact automatic tasks even they can be integrated with third-external applications.

In the next section a case study which shows how to carry out the integration of ISG with processes for the identity management of an entity engaged in development of projects of R&D.

IV. CASE STUDY

In this case study we show how to automate the ISG by means of a BPMS particularly BonitaSoft environment [11]. The case study focuses on an entity which needs to implement an adequate identity management procedure to accomplish with current regulations such as article 93.3 from RD 1720/2007 from Spanish Government: “When the authentication mechanism is based on password must have a procedure to assign, distribute and to store which guarantees the confidentiality and the integrity.” Furthermore, ISO/IEC 27001:2013 standard requires the definition of a control about the rights access revocation and reassignment at procedure A.9.2.6. These business goals enable ISG to ensure the achievement of maturity level 4 maturity according with the required at ISO/IEC 21827:2008.

The two main drawbacks have been identified are: firstly it is the time of registration process since it is too long; secondly passwords have been chosen by the users are usually so weak, up to the point that in several occasions privacy and confidentially has been compromised. All processes to support the tasks for the identity management at the entity have been carried out manually without monitoring mechanisms. In order to improve those processes the entity has proposed to automate the identity management by using a BPMS. Therefore the goals of this project are the following:

1. The compliance of the particular policies (95% of total passwords comply the established rules) and ISO/IEC 27001:2013 by means of the implementation and deployment of the corresponding processes for ISG in a BPMS.
2. Once deployed must be carried out simulations to check the compliance of the following SMART (Specific, Measurable, Achievable Relevant and Time-targeted) objectives [12] proposed by the ISG:
   a. Current user registration process takes at least 3 days from user/password is requested until is received. Users (researchers, administration staff, and third parties) by the time they are contracted, they are added to the Human Resources (HR) database which contains all the users. On the other hand, there is a LDAP database in the Communications Administration Service which contains all users used by other applications. The entity pursues to improve the time of user/password assignment in 60% from the submission until reception.
   b. The relation of users that exists daily in HR and LDAP database is 1.0 and all the users in LDAP database are in the HR database.

The entity has identified various critical assets in form of groups and roles of people who take part in and the processes that are involved such as shown in Fig. 2. The processes to registration, assignment, and revoke user/passwords are well defined and structured. These two processes are shown in Fig. 6-8 at the Appendices.

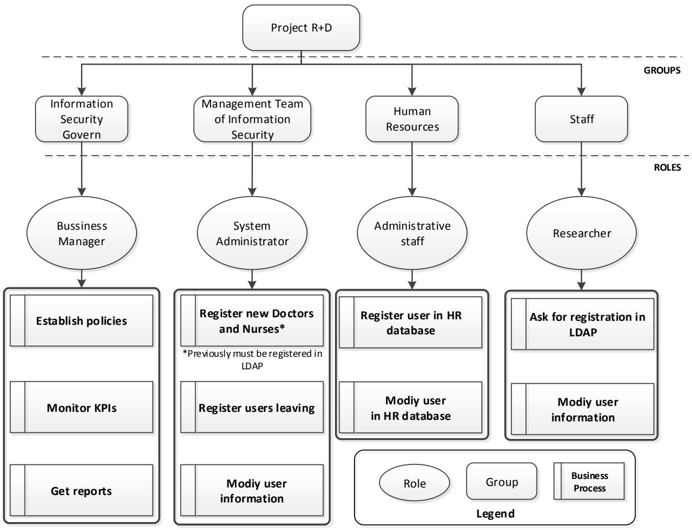


Figure 2. Roles, groups and business processes of the entity.

The ISG has directed these requirements by means of:

- Defining a set of metrics (Key Performance Indicators, hereinafter KPI).
- Proposing a set of particular policies.
- Requesting reports to see the compliance of the established metrics.

A. *Establishment of KPIs*

The KPIs establishment requires a previous work for the ISG that enables the metrics how, what, and when must be defined. In this case, we propose to use a template such as proposed in ISO/IEC 27004:2009 [13] where the most relevant information about the metrics can be established. Templates are a formal, organised and systematic way to define a metrics since the most relevant information is established in that template such as controls to be carried out or the decision criteria has to be applied. An example metrics definition looks like as following Table 1, where a KPI is defined to measure the password quality in the registration process for the entity.

Once the KPIs are defined, the ISG has to introduce that information in the systems by launching the Direct ISG process.

B. *Direct ISG process*

In Figure 7, the business process shows the control-flow which is composed of two sub-processes:

1. A manual process that enables the ISG two options: to establish a new policy and to evaluate a metrics.
2. An automatic process where metrics (KPI) are collected and reported monthly.

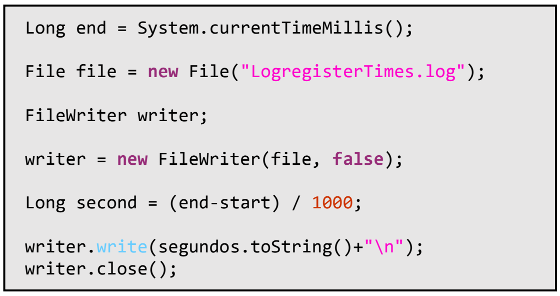
The entity needs to establish a policy to check possible discrepancies between HR and LDAP databases. Firstly, in order to define the policy the role in charge, login at the system and automatically provides the available options: “Register a new policy" or "Check a KPI". In this case, a specific policy wants to be established and a web form is given to establish the policy such as shown in Fig. 8. The form is prepared to pick up all the parameters required in the control. Once "Send" button is clicked on all those values are stated in a database of policies. This database is used as the basis to check the decision criteria of compliance or non-compliance during the registration process.

Table 1: Example of KPI formalization

KPI	
Name	LDAP and HR database discrepancies
ID	KPI-003
Purpose	To assess the quality of the authorized users
Goal	Check whether users registration process in the organization is conform to Control Objective A.9.2.6 in ISO 27001:2013
Measurement Specification	
Objects of Measurement	1. LDAP database 2. HR database
Attributes	1. Number of users in LDAP database 2. Number of users in HR database 3. Id. of users that are not in LDAP database 4. Id. of users that are not in HR database
Basic measures	1. Registration in LDAP 2. Registration in HR
Method	1. Check for each entry in LDAP database whether it is contained in HR database. 2. Check for each entry in HR database whether it is contained in LDAP database.
Measurement type	1. Objective measure 2. Objective measure
Scale	1. Integer value 2. Integer value
Scale type	1. Cardinal and text. 2. Cardinal and text.
Measure unit	Amount of users and identifiers of users.
Indicator Specification and Reporting	
Description	a) Conformity Ratio b) List of non-authorized users.
Analytical model	a) Divide the total number of users in LDAP database by total users in HR. b) Select the users that are in LDAP database but not in HR database.
Incdicator Interpretation	a) Resulting ratio should be 1.0 to meet the control objective satisfactory b) List should be empty for meeting the control objective satisfactory
Reporting Format	A dashboard with charts where the amount of users registered in each database are represented and the list of id. of users that are in a LDAP database but not in HR database.
Reporting Client	ISG Team
Collecting Frequency	Each registration user
Analysis Frequency	Daily
Reporting Frequency	On demand of ISG team.

C. Monitor process

Monitoring of KPI implies to include an imperceptible piece of software (BonitaSoft connectors) in the processes that allows collecting information during the execution of processes. For instance, regarding the time of registration of a new, two timestamps are logged: the first check-point is released when a registration process is initiated, and the second check-point is released when the user has received a response from Human Resource (HR) Department and LDAP. This information is dumped in a database prepared for KPIs. On the other hand, regarding the quality of passwords a validation script is prepared to be performed through all users' registration. An example of Groovy script is shown in the Fig. 3. This piece of script shows a mechanism to write the log registration time.



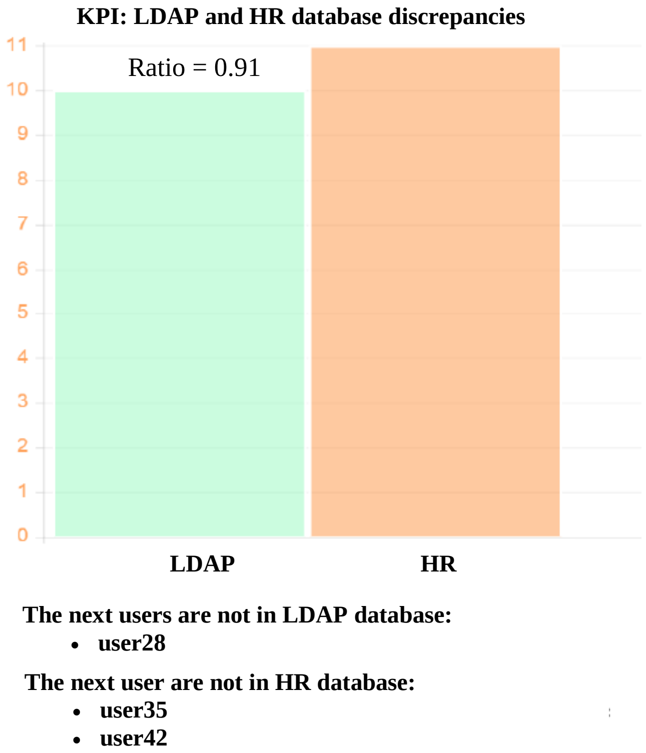
```
Long end = System.currentTimeMillis();

File file = new File("LogregisterTimes.log");

FileWriter writer;

writer = new FileWriter(file, false);

Long second = (end-start) / 1000;

writer.write(segundos.toString()+"\n");
writer.close();
```

Figure 3. Example of Groovy script

Another script enables to count the number of non-compliance against the compliance and stated this value in the database of KPIs. The other KPIs are developed in the same way, that is by means of Groovy scripts where timestamps are stated and queries to database are needed to check the required time of the registration process.

D. Evaluate process

The evaluation of KPIs can be carried out in two directions: manually and automatically. Manually by means of the options provided to the ISG within Direct process or a monthly report is generated. As a result of the monitoring of processes a dashboard can be presented to the governance such as shown in Fig. 4. In the bar chart we can observe the number of users registered in LDAP (blue colour) and HR (yellow colour) database. In this example we can observe a non-compliance example which a discrepancy is shown due to one user that is in HR database but is not registered in LDAP database. In that case the chart is showing. Therefore, the ISG can peek the compliance of policies in seconds at real-time.


KPI: LDAP and HR database discrepancies

The next users are not in LDAP database:

- **user28**

The next user are not in HR database:

- **user35**
- **user42**

Figure 4. Example of dashboard.

V. Conclusions and Future Work

In any organization the importance of ISG is emerging as a key factor in the assurance and protection of information. To build on developments of information security practices, research in effective governance processes that can be aligned with these practices has been undertaken.

BPMS offers a framework which helps to assess and implement this ISG component of information security. It was analysed and applied to the identity management of users/roles for the ISG/ISM in the development of R&D Projects in a Research Group of a Spanish Foundation. This implementation provides a framework of different processes to perform the information security governance (evaluate, direct, monitor, and communicate). These processes show the adequate integration between governance and management of information security.

As future work, we propose to expand the scenarios for ISG/ISM in order to achieve the same goals but collaborating several enterprises or organizations

References

[1] INCIBE, Available at: https://www.osi.es/gl/actualidad/avisos/2011/10/sony-bloquea-93000-cuentas-de-su-playstation-network, 2015.

[2] SIGMA DATA SECURITY CONSULTING S.L., Estudio sobre el cumplimiento de la LOPD por la PYME Española, 2010.

[3] ISO/IEC 27001:2013, - Information security management.

[4] Rossouw von Solms, S.H. von Solms, Information Security Governance. Springer, 2009.

[5] ISO/IEC 27014:2013, Information technology — Security techniques — Governance of information security.

[6] COBIT 5 for security information. ISACA 2012

[7] Jacques Coertze, Rossouw von Solms: A software gateway to affordable and effective Information Security Governance in SMMEs. ISSA 1-8, 2013.

[8] Rahul Rastogi, Rossouw von Solms: Information Security Governance: A Re-Definition. IICIS 2004: 223-236, 2003

[9] Rossouw von Solms, S.H. (Basie) von Solms: Information Security Governance: A model based on the Direct–Control Cycle. Computers & Security 25: 408–412 2006.

[10] Howard Smith and Peter Fingar. Business Process Management (BPM): The Third Wave. Meghan-Kiffer Press.

[11] Bonita Soft, Available at: http://www.bonitasoft.com, 2015.

[12] Business Motivation Model v1.1 OMG 2010

[13] ISO/IEC 27004:2009, Information technology. Security techniques. Information security management — Measurement.

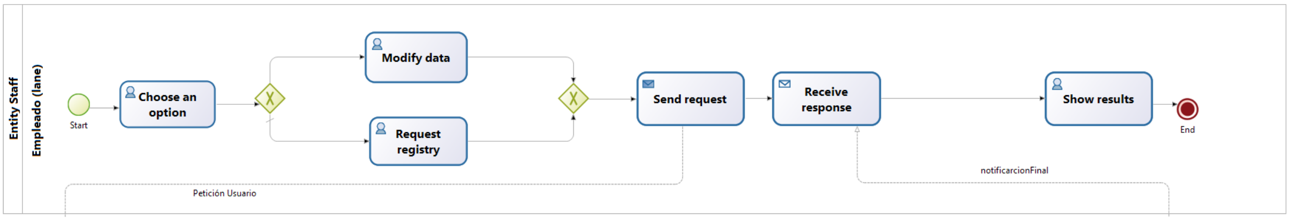


Figure 5. Registration process in the entity.

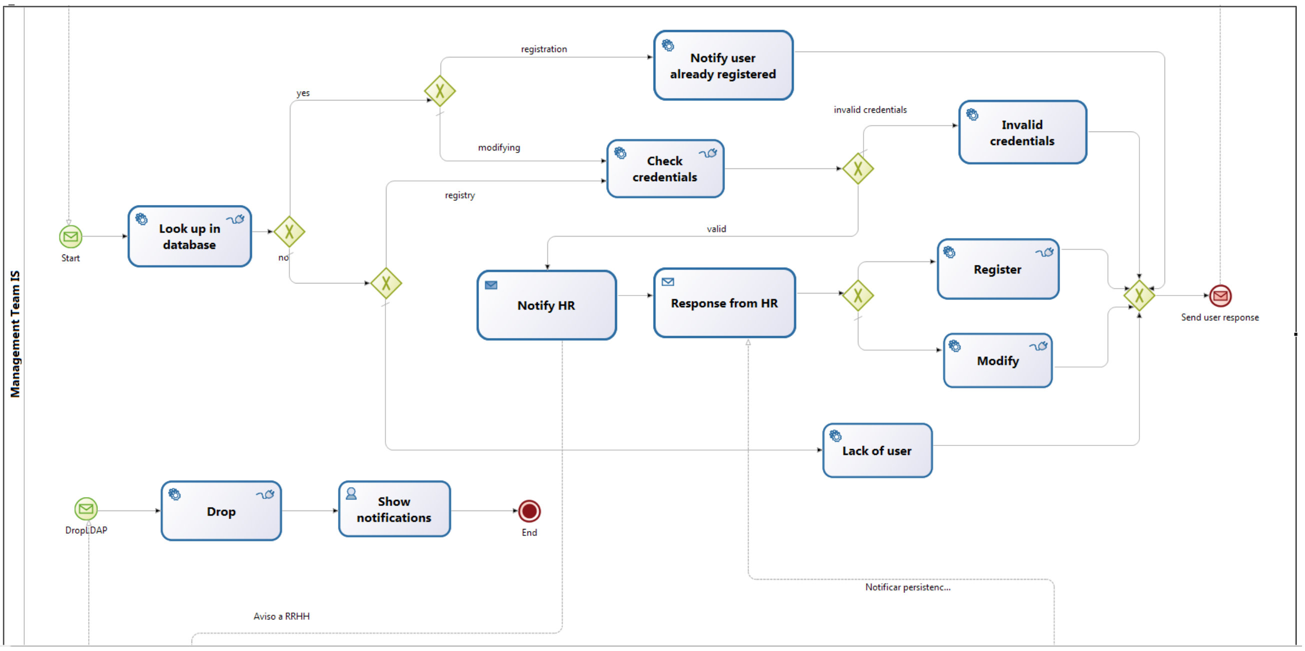


Figure 6. Log process of registration, modification and unregister of a user.

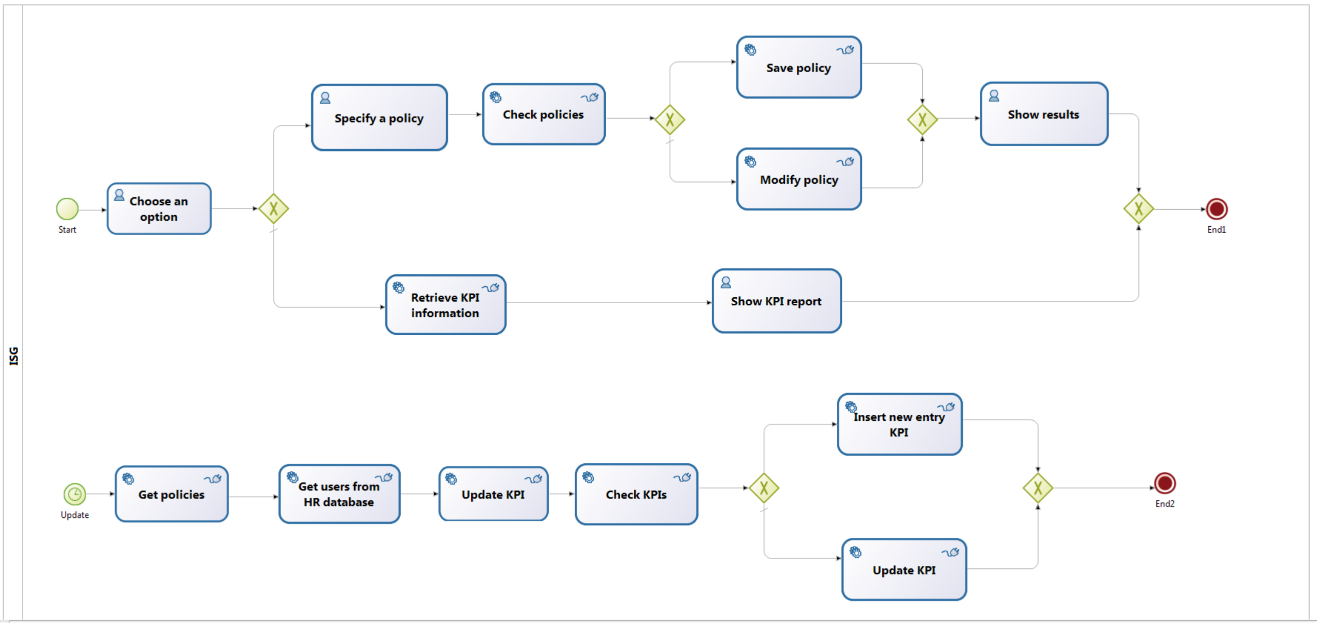
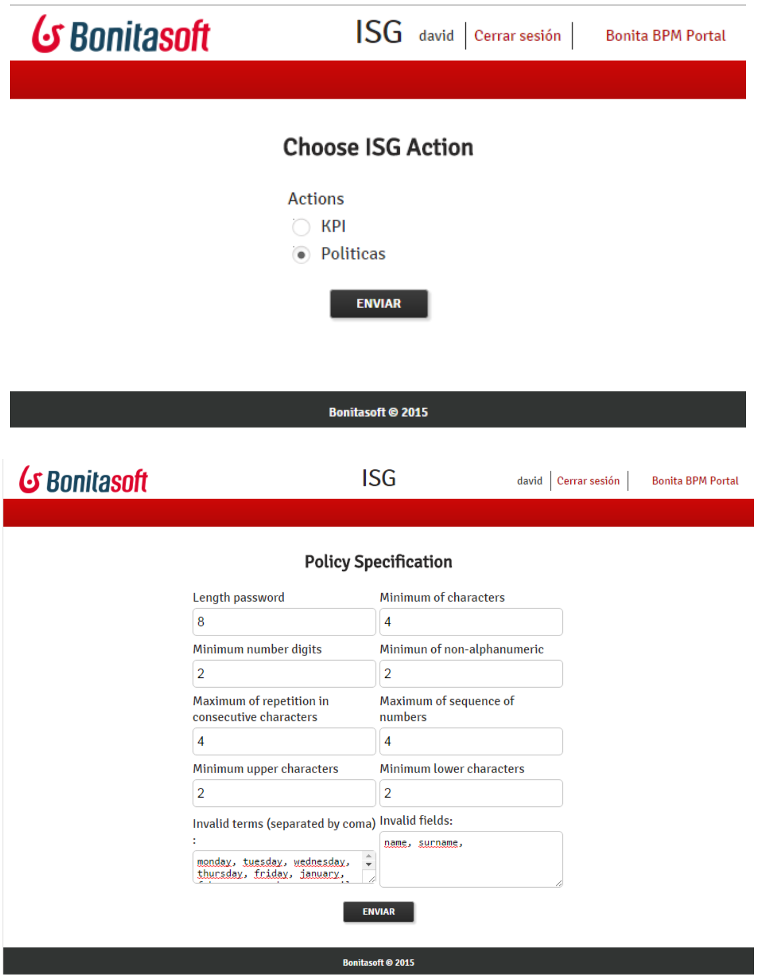


Figure 7. Direct Process for the ISG.



Choose ISG Action

Actions

○ KPI

● Politicas

Policy Specification

Length password	Minimum of characters
8	4
Minimum number digits	Minimun of non-alphanumeric
2	2
Maximum of repetition in consecutive characters	Maximum of sequence of numbers
4	4
Minimum upper characters	Minimum lower characters
2	2
Invalid terms (separated by coma) :	Invalid fields:
monday, tuesday, wednesday, thursday, friday, january,	name, surname,

Figure 8. Example of web form to establish a password policy.