Risk Management Pilot for SMEs and Micro Enterprises in Spain

Final Report

Prepared by:	GMV Soluciones Globales Internet		UNCLASSIFIED
Checked by : :	N/A	Code	SGI-ERNSTING-INF-005
Approved by :	Mª Teresa Avelino Carmona	Version:	1.1
Authorized by:	Mª Teresa Avelino Carmona	Date:	05/01/2009

GMV SOLUCIONES GLOBALES INTERNET S.A.
P.T. Boecillo Parcela 101 - 47151 Valladolid.
Tel.: +34 983 54 65 54, Fax: +34 983 54 65 53.
www.gmv-sgi.es, www.gmv.com.
Secure e-Solutions.

Internal Code: GMVSGI 21027/08

-THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY-.

DOCUMENT STATUS

Version	Date	Pages	Text Processor	Changes
0.9	25/11/2008	33	Word 2007 English	Advanced Draft
1	12/12/2008	52	Word 2007 English	Comments replied and sanitized reports incorporated
1.1	05/01/2009	54	Word 2007 English	Executive Summary rebuilt and further comments reviewed. English translation reviewed.

INDEX

LIST OF TABLES AND FIGURES

1. EXECUTIVE SUMMARY

The RM Pilot for SMEs and micro-SMEs in Spain has given the opportunity to all participants to start using the simplified Risk Assessment and Management approach described in the ENISA deliverable: Information Package for SMEs – Please see References Annex for further information about this Package.

Most of the Risk Management experiences in Spain come from the Official organisations, who rely on Magerit Methodology. This is also the methodology of reference for most of the biggest companies, as they usually collaborate with the Administration.

However, there was no tool available or at least not recommended for Small and Medium Enterprises. As a consequence of it, most of them did not know how to take decisions related to investment in IT Security.

As this report is intended to explain in detail the RM Pilot in Spain, it will start telling the reasons that moved both ENISA and rest of participants to go on with this project.

Then, it will be described the criteria followed for SMEs selection, including a brief description of each SME and the characteristics that made them valuable for this RM Pilot.

After this introduction, it will be shown the activities accomplished and developed of the Pilot in terms of meetings, follow-up actions and progress schedule.

It is also offered information from Workshops held within this Pilot and another related dissemination activities such as ENISE Workshop.

Another issue of great importance dealt in chapter 3 is related to the Methodology deployment over the Pilot. It is explained the reasons for the choices made in order to fit both to the characteristics of the enterprises but also to the RM tool used.

In chapter 4 it is discussed in detail the troubles found using ENISA Methodology approach and it has been suggested a number of modifications regarded as of interest.

Results of the Pilot in are presented in chapters 5, 6 and 7. First it comes a general overview of the experience from GMV's point of view as RM outsourcers and then there come the comments made either explicit or implicit by SMEs and rest of participants – RM tool provider, CEEI and overall comments taken from workshops.

Chapter 7 is devoted to Feedback from companies, which is the most interesting result of the report and measures the satisfaction obtained by SMEs and micro SME involved. It is included a review of comments translated to GMV and regarded of interest.

Finally, the working documents used within the project – Questionnaires, RM reports – Sanitized due to Non Disclosure issues with SMEs involved – are presented here.

As an overview of the findings of this pilot, here are the most important points dealt throughout the last chapters:

- **SMEs take decisions related to technical solutions implementation mainly using a cost-benefit analysis of safeguards**. They usually think only on a near future scope and focusing only on understable and really very provable threats. This analysis is not currently managed by ENISA approach.

SMEs try to save as much money as possible when looking for safeguards implementation. So they demand help in finding costless or very cheap solutions, which is out of the scope of the methodology approach.

We consider that Risk Management tasks should be complemented with these two key elements:

- Previous widespread awareness of Board of Directors of SMEs on Risk Analysis and Risk Management no matter the methodology applied.
- The RM report should be accompanied by a guide on how to implement safeguards.
- A set of references and documents and websites of interest to enhance their knowledge about RM but also about security best practices.

2. INTRODUCTION

2.1. BACKGROUND OF THE PILOT

Over the last ENISA's event on Risk Management that took place in Barcelona, November 2007, it was hightlighted the lack on Risk Management culture among Small and very Small enterprises.

There was also reported the absence of motivation in introducing IT security and Risk Management and requested targeted activities to enhance this ground on IT security for small and micro enterprises.

Despite some reports that echo an increasing investment in technology by Spanish companies and a reasonable concern about security measures to protect their business assets, it is clear that most companies, specially the smaller ones, are not used to Risk Analysis, Business Impact Analysis or in some cases any Analysis at all. That means that they are purchasing security solutions in blind fashion.

In its efforts to promote Risk Management and Information Security, ENISA has generated a methodology approach based on OCTAVE, aimed to help small enterprises (SMEs) to understand and to apply Risk Management. (See ENISA Deliverables mentioned in the References chapter: "Information Package for SMEs" and "RM&IT Security for Micro and Small Business·

2.2. OBJECTIVES OF THE PILOT

One of the major ENISA's goals is promoting the Information Security Awareness.

In order to achieve this objective, ENISA Work Program for 2008 has included a preparatory activity with the title "**Building Information Confidence with Micro Enterprises**".

Within this activity, it was regarded a number of pilots (initially four) to be performed during present year to check the applicability of available ENISA results in the area of Risk Management for Small and Micro enterprises.

With these pilots ENISA would like to promote Risk Management among this type of enterprises.

The pilot was regarded to be performed in cooperation with a promoter organization that should guarantee the incorporation of a potential set of small and micro enterprises.

In our case, the CEEI – That stands for Center of European Enterprises in Castilla-Leon area – was contacted by GMV to participate in the Pilot.

The industrial team participants showed **different interests and motivations** for participating in the pilot:

GMV, as a professional services firm in the information security industry, has had the opportunity to test and train its consultants in ENISA's risk assessment and management methodology for SMEs, as well as to analyze the market for potential customers.

CEEI, as a public owned (Junta de Castilla y León) company who focuses on SMEs fostering and innovation, has offered to its base costumers (SMEs) the opportunity to introduce risk management process, being aligned in this way with similar activities encouraged by different local and national organisms such as for example INTECO's SGSI adequacy for Small Companies.

A.L.H.J Mañas S.L has contributed to this pilot as RM tool provider: **Pilar Basic**.

P.D. Jose Antonio Mañas is a prestigious professor in the Politechnical University in Madrid and has developed several Risk Management tools such as Chinchon, EAR or the standard PILAR tool that is aimed for Magerit Methodology.

A.L.H. J. Mañas S.L. has been able to adapt ENISA risk management modules for PILAR Basic RM/RA Tool, gaining insight and understanding regarding tool usability and performance and also analyzing applicability for new potential clients.

Finally, for the four **SMEs** participating in the pilot, they have had the opportunity to have implemented risk management process following a full-outsourcing scheme taken by GMV. They also have had the opportunity to be taught about Risk Management in general, good practices and Risk Management maintenance through the adapted tool PILAR

2.3. SELECTION OF THE SMEs AND MICRO ENTERPRISES

The selection was made by GMV –Soluciones Globales e Internet S.A delegation in Boecillo with the support of CEEI.

The CEEI is the European Centre of Enterprises in the Castilla y Leon Area. It plays the role of facilitator for all the Small Companies that want to set up in this area. They are offered a place inside any of the CEEI buildings. They also get from CEEI some basical services as common reception and security guards or even a small canteen.

CEEI also promotes among its members support for innovation and growth. As this Pilot was regarded as an initiative in line with Security Awareness and Certification promoted by National Organisms, they collaborated by providing a grouped and vast number of companies with the desirable characteristics, among those of which the following ones were finally selected as they also show interest and can allocate resources in order to participate in the PILOT.

-

Category	Company Name	Activity
SME	**Instituto Biomar S.A.** http://www.institutobiomar.com/	Chemical and pharmaceutical industry
SME	**Machine Point, S.L.** http://machinepoint.com/	Industrial Machinery e-business
Micro-SME	**Próxima System** http://www.proximasystems.net	Industrial software
SME	**Besel S.A (Boecillo)** http://www.besel.es/	Technical Consulting Services on Renewable Energy

Table 1: SME selection

As it can be seen, those companies belong to different areas of interest, and make a reuse of IT technology but do not develop it by itself. So, for them, IT resources are a key point in achieving their business objectives though not the objective itself.

Instituto Biomar S.A is a company that is devoted to the discovery and development of new bioactive compounds from marine microorganisms.

Their development process starts with the collection of marine samples. Then, it is followed by the isolation of microorganisms from marine invertebrate and algae, and their analysis. Finally, they proceed to the study and identification of active secondary metabolites and further production of large amounts of them for commercial purposes.

They are also interested in forming productive collaborations with pharmaceutical, chemical, cosmetic and environmental companies to exploit its technology for product development and commercialization.

SoIT is an important tool for their development processes to ensure control and record of everything of interest.

Although their current Production Plant is located in Leon, inside Onzonilla's CEEI premise, they have plans to move in near future to a bigger laboratory.

So for them, it was an strategic goal to have done a Risk Assessment and further Business Continuity Plan, before moving.

Machine Point S.L is an international trading company specialized in selling second-hand machinery in the plastic sector.

They have contacts with more than fifty countries and their expertise lies in machinery for the film extrusion and converting; extrusion of pipes, tubes and profiles both rigid and flexible; PET performs, bottles, filling lines for soft drinks and water, disposable food packaging, packaging for the dairy industry, molded parts, compounding and thermoplastics recycling.

As they advertise their products or call for potential sellers in their Website and make e-Business, IT has become a critical point in their day-to-day business.

They are located in CEEI premises in Boecillo –Valladolid and have an own IT department compound of three qualified technical administrators.

Although they arrive to this Pilot by mistaking Risk Management with ISO 27001 certification, they admit being quite satisfied with the experience, as they have now reached an understanding of the Risk Analysis process and also of their own Business Processes that they do not have at the beginning. In addition, they have become the more proactive among the four studied companies in this Pilot and also showed their will to go on collaborating whenever is possible.

Proxima Systems S.L is specialized in industrial applications of Information Technologies.

There are mainly development solutions in the following areas:

- Remote monitoring and telecontrol of industrial processes, buildings, etc.
- Intelligent video surveillance over heterogeneous data networks.
- Industrial computing automation.
- Integration of hardware, networks and software in industrial and corporate environments.

This is the micro-SME studied and they are only nine people altogether. The average staff profile is a young but high-qualified engineer.

Besel S.A

Besel is a company specialized in the state-of-the-art for energy and environmental technologies.

Besel Consultancy solutions located in CEEI premises in Boecillo –Valladolid include:

- Technical and strategic consultancy.
- Process innovations and continuous improvement planning.
- Planning, management and development of projects.
- Training, awareness campaigns and publications.

On the following fields:

- Energy savings and efficiency
- Renewable energies
- Environment
- Mobility & Transport

For this company, IT is a key point in the SCADA processes. **SCADA** stands for Supervisory Control And Data Acquisition. It generally refers to an industrial control system: a computer system monitoring and controlling a process. The process can be industrial, infrastructure or facility based. In this case, it is related to infrastructure, which contains most remote terminals that send to a control point the information related to certain processes as for example, the water treatment. So Besel offers knowledge for setting these control points.

They rely much about IT technology, especially everything concerned with remote controlling, networking with remote terminals and therefore security is something they have in great concern.

2.4. PLANNING AND ORGANISATION OF WORK

During the deployment of the pilot, the following meetings were held:

- **Kick-off Meeting :** Held on the 14th July in GMV premises in Madrid.
  - Participants were ENISA, GMV and **A.L.H. J. Mañas S.L**

During this meeting, it was made some agreements over the overall procedure to be followed up and was formally accepted the proposal sent by GMV in response of the call for participants made by ENISA .

Basic aspects of the Pilot were discussed and scheduled such as:

- Preparatory Workshop preparation, dates, participants, materials, etc.
- Final Workshop rescheduled to mid November to have enough time for preparation and feedback from SMEs
- Customizing of Pilar Tool to be used with ENISA methodology approach.
- Regarded dates for intermediate progress reporting by GMV.
- Procedure with each SME for Risk Analysis development.
- Training for the GMV team on Pilar with ENISA methodology new library.
- Translation of documents of interest for the Pilot.
- Dissemination activities foreseen to widespread such as ENISE II event articles in technical journals

- **Training Session on PILAR + ENISA library :** Held on 1st September in GMV premises in Madrid.
  - Participants were GMV Risk-Management team in the project and J.Mañas, who was the trainer.
  - Over the training some assumptions were made related to methodology approach for development the Risk Analysis on every SME. (See chapter 3).
  - GMV team asked J.Mañas to make further modifications to reflect better ENISA methodology. Modifications were scheduled for the following week as work with SMEs were to be in time.
- **Preliminary Workshop:** Held on 4th September in GMV premises in Boecillo.
  - Participants were GMV (Risk Team + Managers who have collaborated in SMEs selection), J. Mañas, CEEI, Machine Point (2 IT responsible), Proxima Systems (Manager).
  - Over this workshop, participants were presented to each other and GMV Risk Team explain the reasons and goals of the Pilot, how it was going to be carry out in terms of effort required to every participant, provisional dates for meetings, legal aspects to be bear in mind, deliverables, feedback required and possible dates for Final Workshop.
  - SMEs presented their business needs in terms of security. T
  - A basic introduction on Risk Cycle of life was presented by J.Mañas as we noted none of the SMEs have a clear idea on this matter.
- **Meetings with every SME:**

- A devoted meeting was arranged with every SME, with an average duration of three hours – Four hours for the two companies who have not been able to attend the Preliminary meeting.
- Meetings were in every SME premises including a tour of more or less twenty minutes to have evidence of basic aspects of Physical Security, Staff habits, and business development in a day-to-day basis.
- The calendar for the Risk Analysis first interview was as follows:
  - **11th September: Machine Point S.L and Proxima Systems S.L**
    - We took advantage of the close location of both of these two companies to our GMV premises in Boecillo. So we managed to spend three hours with each one that day and afterwards the IT RM team had an internal meeting in GMV premises in Boecillo to discuss over information obtained.
    - In the case of Machine Point S.L we interviewed the IT department at a whole (3 members) + occasional questions to selected staff by the IT members when appropriate.
    - In the case of Proxima Systems S.L. (micro-SME) we interviewed the manager and Technical Developer responsible and also the IT administrator.
  - **16th September: Besel S.A.**
    - We devoted the whole afternoon to this company, making an introduction to the Pilot, Risk Management and Pilar Tool as they were unable to make the Preliminary Workshop.
    - We interviewed the IT manager and also for some technical issues, two consultants who were appointed by the IT Manager to answer some questions that arose in the middle of the Risk Analysis.
  - **23rd September: Biomar S.A**
    - We interviewed the Product Manager and some staff: Researcher in charge of main projects, and also some administrative personnel.
    - We also provided them an introduction to the Risk Analysis, the ENISA Pilot grounds and Pilar Tool.

After every Risk Analysis was made further doubts were answered by phone by designed point of contacts provided during the first interview.

E-mail was only used to arrange new meetings or any other issues not related to confidential information as NDA was signed by every party in the first meeting and procedures were clearly stated.

- **Report delivering and discussion with every SME:**

After reports were finalized and all doubts were clear, we arranged again meetings with every Point of Contact designed for this task that was also present in the meeting for carrying out the Risk Analysis.

During these final meetings, in addition to handled them in a confidential way, the deliverables we discussed with them the results, the recommendations and about all, we had again their feedback about the experience.

We also helped them to install Pilar Tool – As we also included in the deliverable package their license file provided by J.Mañas.

We also reviewed with them the file with their report in Pilar format and teach them on how to maintain that file updated for their Risk Analysis report.

Finally, we showed them how to obtain reports from the tool and what information was put on these reports so they can have a useful dossier for Board of Directors decisions supporting.

On average, we devoted one hour and a half on every interview.

The deliverable package consisted on a bounded report printed in color with their Risk Analysis Report and a CD containing the same report in pdf format, the installation file of Pilar Tool and their license file. We also included the final questionnaire in doc format so they can modify it and give it to us back easily.

- Meetings scheduled:

  - 29th September: Machine Point S.L and Proxima S.L.
  - 6th October: Besel. S.A. Matrix premises in Madrid.
  - 8th October : Biomar. S.A. Manager's private Desk in Madrid.

Although it was said to SMEs to give back their answers in ten day's time, it took them up to the first week of November to send us their feedback. Some of them claimed that it tooked some time to become used to the Pilar Tool but some others were only because of lack of time for this task.

There was even a SME – Besel.S.A – Which was reluctant to give an answer and finally sent it to us after more than three weeks after we gave them the deliverable package.

It must to be mentioned that this company has many other locations in Spain and the Point of Contact they gave us – IT manager - was commuting from one location to other quite often, what was quite a nuisance for us because it delayed the feedback task collecting.

- **Meeting with J.Mañas to have his feedback over the Pilot:** 23rd October in Leon.

  As we were invited by INTECO to participate on ENISE II event with our experience with SMEs and new ENISA approach - see references made and agenda in this website:

  - https://2enise.inteco.es/component/content/article/99-agenda-t32

  So we met up the evening before the event premises to coordinate our presentations – and discuss over the Pilot experience with most of the feedback already provided by SMEs.

We also discussed on how to enhanced the tool and also ENISA approach to satisfy the requirements made by SMEs.

On the 24th, we made dissemination on the ENISA approach, how the procedure with SMEs has looked like and overall result so far. J.Mañas show how Risk Analysis for a SME could be easily carried out through PILAR tool with ENISA library provided.

- **Final Workshop:** Held on the 10th of November, in GMV premises in Boecillo.

  - Participants: ENISA, GMV, CEEI, J. Mañas and Machine Point S.L.

During this final meeting, GMV offered a presentation with basic results on the feedback made by companies, which were clarified by Machine Point S.L whose IT department participated in quite a proactive way, providing explanations to some issues observed related mainly to lack of previous knowledge on Risk Analysis and also with feeling a bit insecure about handling Risk Analysis.

There were also positive comments about the improvements on their business processes and to the whole company provided by the methodology. They also admitted having worked before in a numbness way with reference to Risk handling although they express they have been always interested in Security.

Although Proxima Systems S.L could not participate in the project, they express their wish to go on participating in any other initiative promoted by ENISA and so did Biomar S.A.

Both Proxima Systems S.L. and Machine Point S.L. had requested GMV for information related with local initiatives in similar issues such as the INTECO SGSI project for SMEs.

ID	Nombre de tarea	Duration	Start	Finish
1	**ENISA Risk Management Implementation Pilot**	**100 days?**	**Mon 14/07/08**	**Fri 28/11/08**
2	**Kick-off Meeting**	1 day	Mon 14/07/08	Mon 14/07/08
3	**Activity 1 Project Management and Product Assurance**	**44 days**	**Fri 01/08/08**	**Wed 01/10/08**
4	**Progress Report Submission**	**44 days**	**Fri 01/08/08**	**Wed 01/10/08**
5	Progress Report Submission 1	1 day	Fri 01/08/08	Fri 01/08/08
6	Progress Report Submission 2	1 day	Mon 08/09/08	Mon 08/09/08
7	Progress Report Submission 3	1 day	Wed 01/10/08	Wed 01/10/08
8	**Activity 2 Preparatory Activities**	**38 days?**	**Tue 15/07/08**	**Thu 04/09/08**
9	ENISA Methodology - Document Translation	15 days	Tue 15/07/08	Mon 04/08/08
10	Training in PILAR & ENISA Methodology	15 days	Thu 07/08/08	Wed 27/08/08
11	Workshop Preparatory Activities (documentation, presentations, etc.)	5 days	Thu 28/08/08	Wed 03/09/08
12	Preparatory Workshop	1 day?	Thu 04/09/08	Thu 04/09/08
13	**Activity 3 Implementation of Risk Assessment Process**	**24 days**	**Fri 05/09/08**	**Wed 08/10/08**
14	**SME#1 Risk Assessment**	**7 days**	**Fri 05/09/08**	**Mon 15/09/08**
15	**Phase 1 - Risk profile selection**	**0,25 days**	**Fri 05/09/08**	**Fri 05/09/08**
18	**Phase 2 - Critical Assets Identification**	**0,75 days**	**Fri 05/09/08**	**Fri 05/09/08**
22	**Phase 3 - Control Cards Selection**	**0,5 days**	**Mon 08/09/08**	**Mon 08/09/08**
26	**Phase 4 - Risk Management and Implementation**	**3 days**	**Mon 08/09/08**	**Thu 11/09/08**
29	**Risk Management Report**	2,5 days	Thu 11/09/08	Mon 15/09/08
30	**SME#2 Risk Assessment**	**5 days**	**Fri 12/09/08**	**Thu 18/09/08**
31	**Phase 1 - Risk profile selection**	**0,25 days**	**Fri 12/09/08**	**Fri 12/09/08**
34	**Phase 2 - Critical Assets Identification**	**0,75 days**	**Fri 12/09/08**	**Fri 12/09/08**
38	**Phase 3 - Control Cards Selection**	**0,5 days**	**Mon 15/09/08**	**Mon 15/09/08**
42	**Phase 4 - Risk Management and Implementation**	**3 days**	**Mon 15/09/08**	**Thu 18/09/08**
45	**Risk Management Report**	0,5 days	Thu 18/09/08	Thu 18/09/08
46	**SME#3 Risk Assessment**	**5 days**	**Thu 18/09/08**	**Thu 25/09/08**
47	**Phase 1 - Risk profile selection**	**0,25 days**	**Thu 18/09/08**	**Thu 18/09/08**
50	**Phase 2 - Critical Assets Identification**	**0,75 days**	**Thu 18/09/08**	**Fri 19/09/08**
54	**Phase 3 - Control Cards Selection**	**0,5 days**	**Fri 19/09/08**	**Fri 19/09/08**
58	**Phase 4 - Risk Management and Implementation**	**3 days**	**Mon 22/09/08**	**Wed 24/09/08**
61	**Risk Management Report**	0,5 days	Thu 25/09/08	Thu 25/09/08
62	**SME#4 Risk Assessment**	**9,5 days**	**Thu 25/09/08**	**Wed 08/10/08**
63	**Phase 1 - Risk profile selection**	**0,25 days**	**Thu 25/09/08**	**Thu 25/09/08**
66	**Phase 2 - Critical Assets Identification**	**0,75 days**	**Thu 25/09/08**	**Fri 26/09/08**
70	**Phase 3 - Control Cards Selection**	**0,5 days**	**Fri 26/09/08**	**Fri 26/09/08**
74	**Phase 4 - Risk Management and Implementation**	**3 days**	**Mon 29/09/08**	**Wed 01/10/08**
77	**Risk Management Report**	5 days	Thu 02/10/08	Wed 08/10/08
78	**Activity 4 Risk Assessment Results**	**37 days**	**Thu 09/10/08**	**Fri 28/11/08**
79	Risk Process Results Analysis	5 days	Thu 09/10/08	Wed 15/10/08
80	Workshop Preparatory Activities (documentation, presentations, etc.)	3 days	Thu 16/10/08	Mon 20/10/08
81	**Final Workshop Celebration**	1 day	Mon 10/11/08	Mon 10/11/08
82	Final Report Preparation	12 days	Tue 11/11/08	Wed 26/11/08
83	**Final Report Submission**	1 day	Fri 28/11/08	Fri 28/11/08

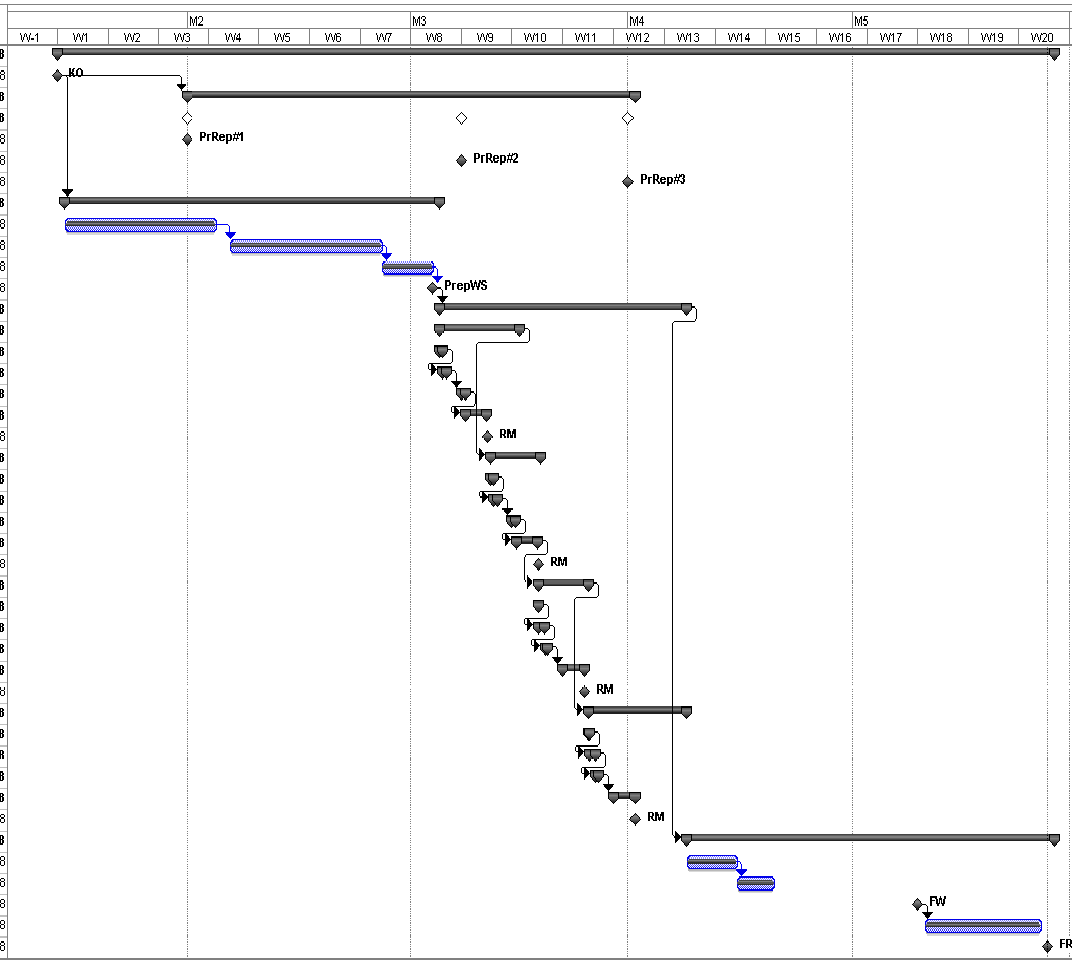

Figure 1: Schedule and Progress

3. METHODOLOGY DEPLOYMENT

GMV is a company with a large experience in Risk Assessment. Our approach to this Pilot was to consider only the outsourced option for carrying out the Risk Analysis in the four companies selected.

This decision was supported by the fact that none of that companies in the database provided by CEEI have been taught in Risk Analysis previously. In addition, they do not have enough human resources to achieve this task even in the case that GMV could give them enough training. However, they should compromise some resources and time for succeeding in this collaboration for the Pilot.

In addition, our experience using **PILAR tool** developed by **A.L.H. J. Mañas S.L** for Risk Analysis using Magerit Methodology, made us also think again on this tool to be adapted to the new methodology.

Before of all, and after being read of ENISA approach through the documentation provided by them, we try to synthesize it in a four-step procedure to be followed-up.

The first step was to determine the profile of the company according to financial, legal, production issues or staff conditions. We try to search about legal considerations that might apply to every company just by checking the area and services that every company was providing. This was done before having the first interview.

As for example, if we read about Machine Point in their website and we realized they contacted potential customers by Internet, then e-Business laws might apply to them or else Personal Data regulations as for example, Spanish laws LOPD or LSSI related to electronic personal data use or spam considerations as well as logs to be kept or any other issues such as privacy, integrity, mail use or so.

We also try to figure out the size of the company – if public information is provided – or if there has been any new posted and related to those companies, that might tell us about incidents, solvency problems or anything of interest.

With previous researched information, we developed both a preliminary questionnaire – See Annex and also a set of possible doubts or questions that might arise during the first interview with the company.

To guarantee privacy of the security vulnerabilities or features that GMV might learn from companies and as part of the code of ethic that GMV has, a **Non Disclosure Agreement** must be signed by both parties – Every SME or micro-SME and GMV – prior to have any non public information about every company.

As the answers to this questionnaire might be regarded as Confidential Data, questionnaires should be used by companies to determine who should be present in the first interview. They must provide information such as how many workers the company have or else how many days without the critical business process the company can stand without a dramatic lost.

When it comes to company profile, a default value meaning **non significant** was added as it was not regarded previously among possible selections. This value will apply when the aspect treated has nothing to do with the company, as for example, financial issues or legal issues, etc.

Once classified the company, there comes the second step in which four types of assets were chosen among all in order to have the most relevant features of the companies.

Time, resources and previous knowledge were factors to be sized before developing our strategic plan that will include at least one extended interview with board of directors or business managers capable of providing us the big picture of their business processes as well as the technical staff in charge of every single process or at least a number of them enough to determine whether certain safeguards have been set or not.

So, just with the large interview, our purpose was to draw a draft on the Risk Analysis that should be adjusted after an overall review and check to determine inconsistencies when answering the questions or any other consideration that might be leave out unnoticed.

On the other hand, apart from making questions related to safeguards mentioned in the corresponding cards, some aspects were reviewed on-site. For example, if we ask them whether they provide security awareness to employees and we notice some issues such as passwords written in post-it notes close to an employee's PC or they usually leave their PC without blocking or things like that, this safeguard is not successfully applied although they claim to. Same for physical security safeguards that can be reviewed easily as we pass through the premises.

4. METHODOLOGY RELATED ISSUES.

4.1. OUTSOURCING OPTIONS

The three outsourcing options offered by the methodology are enough to include every possible situation and circumstances of any SME. Nevertheless, the three set of questions used to determine the right decision may be too repetitive and confusing. Probably, the best option, and the one chose by GMV in the methodology implementation, is to group every different question in one single questionnaire. This simplified questionnaire is the one that the SME should complete. Then, the number of positive answers could easily be mapped into the outsourcing options. The simplified questionnaire used by GMV in the implementation can be found in the first questionnaire of Annex I.

4.2. RISK PROFILE SELECTION

As an overall comment, to our understanding, ENISA **approach for determining the company profile does not take under consideration the three common measurements of the security**, that is : **Integrity, Confidentiality and Availability**. As for example, we can imagine a company that sells its products by Internet, but do not contain in its web any critical information that should not be disclosed. For this company, Availability and Integrity is of great interest but not Confidentiality. However the reverse case could be a company that develops cryptographic material for military purposes and stores particularities of the items developed in a database for accounting purposes with the name of the items, invoicing information, delivery details and the algorithm applied. For them, keeping safe the algorithm used to make the ciphers is critical but not so critical to have available the whole database in a 24x7 basis, however Integrity also must be a important although might be not so critical issue as a mistake in the disclose to end customer could lead to a unsuccessful attempt to communicate through the purchased cipher. However an enemy knowing the algorithm used in the cipher is the most critical issue related to the information.

Taking under consideration the three dimensions of security, would be of interest when selecting safeguards or either when making recommendations about what the target levels should be.

In addition, there are many aspects that could be included in the **risk profile identification questionnaire to obtain a more accurate result**. Most of the subjects dealt in the questionnaire are quite general and so it is no surprise that we obtained nearly the same risk profile for every SME.

In our opinion, **questions related with yearly revenues** could be interesting, but they **are not critical aspects,** especially when the decision limits are five and twenty-five millions and we are talking about SME's. A similar thing happens with Productivity risk area. Although this questionnaire has been used exactly as it's explained in the methodology, many other considerations could be include to identify the risk profile and select then the best safeguards.

Another consideration made that is included in Pilar Tool but not in ENISA approach is the **profile of the potential attacker**. AlThough not every risk is human made, at least it introduces concern about who could have an interest of attacking the company. For instance, in the military case, an enemy country, in the case of a innovative researcher, maybe an industrial competitor or else in any case a discouraged former employee. Motivation to attack is something we consider as of interest at least to encourage companies to make an exercise of self-reflection. Potential attacker will modify the type of threats we can expect and also the threats likelihood.

Such consideration has been included in Pilar tool under the menu "Domain modifiers". It consists in several aspects classified in different categories. Those aspects are taken under consideration when trying to identify the potential attacker profile. The attacker profile will modify the type of threats we can expect and also the threats likelihood. The attacker profile has been mapped in Pilar tool by a multiple selection list with the following options – English translation is provided aside in blue:

Identificación del atacante /Attacker profile
Público en general /General Public
Competidor comercial /Commercial competitor.
Proveedor de servicios /Service Provider.
Grupos de presión política /activistas /extremistas / Political Activists, extremists.
Periodistas /Journalists.
Criminales / terroristas / Criminals, terrorits .
Personal interno / Staff Members.
Bandas criminales /Gangs.
Grupos terroristas /Terrorits groups.
Servicios de inteligencia / Intelligence Services.

Table 2: Potential attacker

Motivación del atacante/Attacker Motivation
Económica /Financial.
Beneficios comerciales /Commercial Benefits.
Personal propio con problemas de conciencia/Staff members with a guilty conscience.
Personal propio con conflictos de intereses/Staff members with conflict of interests.
Personal propio con pertenencia a un grupo extremista/Staff members who belong to an extremist group.
Con ánimo destructivo /With aim of causing destruction.
Con ánimo de causar daño /With aim of causing damaging.
Con ánimo de provocar pérdidas /With aim of provoking financial losses.

Table 3: Attacker motivation

Beneficio del atacante/ Attacker Benefit
Moderadamente interesado /Milded interested
Muy interesado /Very interested
Extremadamente interesado /Extremely interested

Table 4: Attacker Benefit

Motivación del personal interno /Staff Members Motivation
Todo el personal está fuertemente motivado /All the Staff members are strongly motivated.
Baja calificación profesional / escasa formación//Low professional qualification, lack of enought training.
Sobrecarga de trabajo /Work overloaded.
Con problemas de conciencia / Conscience troubles.
Con conflictos de intereses /Conflict of interests.
Personal asociado a grupos extremistas/Staff members associated to extremists groups.

Table 5: Staff members motivation

Permisos de los usuarios/User Permissions
Se permite el acceso a Internet
Se permite la ejecución de programas sin autorización previa
Se permite la instalación de programas sin autorización previa
Se permite la conexión de dispositivos removibles

Table 6: User privileges

Conectividad del sistema de información/Connection to the Information System
Sistema aislado /Isolated System.
Conectado a un conjunto reducido y controlado de redes/Connected to a reduced number of Networks that are under control.
Conectado a un amplio colectivo de redes conocidas
Conectado a Internet

Table 7: Information systems connectivity

Ubicación del sistema de información
Dentro de una zona segura
En un área de acceso abierto
En un entorno hostil

Table 8: Information systems location

Most of the previous aspects provide very interesting information to suggest useful safeguards to the SME.

4.3. ASSET IDENTIFICATION

When it comes to **Critical Asset selection and classification**, it has been difficult to identify the asset category of each critical asset identified, especially when the critical asset is considered as a suit of components, and each of those components is an asset with its own category. As an example we can think on a company which critical asset is an e-commerce application (application category) and whose components are a database, a firewall, a network segment and a server (most of them system category). Each of those components has its own category and probably will require different safeguards depending on that category. Nevertheless, the methodology score card selection will be based only in the critical asset category and will not consider at all the components category. A similar thing happens with security requirements selections since each of the components will have situations different requirements and it should be reflected in the safeguards suggested. In addition, a data or information repository could be useful in some cases and could be easily mapped with access control safeguards, user privileges, etc.

So we introduced some new asset subtypes we have regarded as important such as for example **Printers, PBXs** – They make connections among the internal telephones of a private organization — and also connect them to the public switched telephone network (PSTN) via trunk lines, and therefore, we regarded as of interest in general, not only for this Pilot. This is also valid for **Firewalls**, as regarded also of interest to safekeeping the networks against intruders.

On contrast to ENISA approach, Pilar Tool allows **Asset information to be added,** we took advantage of this feature to add as much information as it was of interest, so also companies can make further use of this feature for inventory purposes or any other plans as for example Disaster Recovery or Asset Maintenance

Asset Category	Asset types
Systems	Printer

Network	Firewall PABX
Applications	Database Management system Office Web server Web client Email server Email client

Table 9: Additional asset types

4.4. CONTROL CARDS SELECTION

Most of the control cards selection considerations are related to the asset classification and have been already mentioned in previous section, nevertheless, another important aspect is threats and their influence. As **ENISA approach does not regard threats,** as Risk Management lifecycle usually do, but as so does Pilar Tool, we decided to select a subset of threats of interest per asset to be used within the Pilot – Not the whole Magerit v.2 set suggested but at least the most common ones. Here it is given the threats we regarded of interest per Asset Category:

Aplicaciones
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.19] Escapes de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.14] Interceptación de información (escucha)
[A.22] Manipulación de programas

Table 10: Threats for Applications

Equipos
[N.1] Fuego

[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.19] Escapes de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.14] Interceptación de información (escucha)
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo

Table 11: Threats for systems

Comunicaciones
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones

[I.9] Interrupción de otros servicios o suministros esenciales
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.19] Escapes de información
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.14] Interceptación de información (escucha)
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo

Table 12: Threats for networks

Personas
[E.7] Deficiencias en la organización
[E.19] Escapes de información
[E.28] Indisponibilidad del personal
[A.19] Divulgación de información
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)

Table 13: Threats for people

However, we found that Pilar Tool does not take under consideration **modifiers for threats likelihood**. It is something we regarded as of high interest as not every company has the same probability of suffering the same problem.

Imagine for example that we pay attention to physical threats to a database server. It is not the same if the company is a laboratory that deals every day with flammable or chemical substances – as for example Biomar S.A than a company that is located in a controlled place and only manages current desk materials – as for example Machine Point S.L. So in the same way, the likelihood of fire damage as a threat to the asset regarded is not the same for both cases. In the first case, we should recommend higher fire protection measures and, in the second case, only standard measures.

Pilar tool also adds, plus to ENISA recommended, **additional safeguards**. Those safeguards were chosen from the suit provided by the methodology but not directly extracted from the score cards mapping. We also try to keep them as short as possible and, in order not to introduce confusion in the reports we provided them in a separate chapter, noting that this was additional safeguards recommended by the tool and not by ENISA. In addition and using our expertise, we also by means of the Executive chapter in the report, add some understandable recommendations so board of directors could easily read this summary and pay attention to these overall recommendations.

Report generation and risk map charting : Using Pilar Tool have also provided fully reports using a standard GMV pattern for reports. Reports, graphics and reporting tools are useful to give Board of Directors a quick and easy view of the Risk status, targeted levels, areas where lacks have been detected and points to improve.

As a consequence of every previous aspect, especially those explained in asset identification section, it is possible to identify specific safeguards that are not directly extracted from the score cards mapping but from the combination of GMV experience, attacker profile identification, critical asset subcomponents classification and specific SME security issues identification. In addition, those safeguards were chosen from the suit provided by the methodology as a next recommendable step on a continuous improvement cycle.

4.5. IMPLEMENTATION AND MANAGEMENT/ GAP ANALYSIS

Related to the methodology safeguards, we would like to notice that **some safeguards proposed are a bit too long to fully catch the meaning**. As a recommendation, **cutting them into smaller pieces and giving more examples of application could be of high value for SMEs**. We have had to make an effort to translate in practical some safeguards and only after we provided some examples they understood the meaning.

Pilar tool allows using degrees of setting of safeguards, which is extremely useful in order to simplify the gap analysis understanding. We have evaluated the maturity level for each control in five levels plus the **Non Applicable** one, where the safeguard regarded does not have to do with the company. We have done a gap analysis considering de current situation based on the meeting held with SME against the target situation based on GMV experience. The levels used to identify the maturity of each control are the followings:

- L0. Non Existent → That means that the safeguard is not even regarded, nor set
- L1. initial /ad hoc → The safeguard is not set, but is regarded, planned or partially set
- L2. Reproducible but intuitive. → The safeguard is set but not under a clear procedure
- L3. Defined procedure → The safeguard has been set and there is a clear procedure, with documentation
- L4. Managed and measured → The safeguard is set, has a clear and documented procedure and its presence and efficacy is measured and controlled.
- L5. Optimized → All the points in L4 plus optimized, that means that after measuring and control it has been improved to its maximum efficiency.

5. GMV'S GENERAL COMMENTS AND OBSERVATIONS

At this point, some general comments and observations are made, based on the RM Pilot experience.

Although every company was previously contacted before to be selected in order to know about the Pilot and the objectives of it, companies have **little or even mistaken idea about the Risk Management concept**. Moreover, **none of them have read about ENISA** or any related international institution They have only known about local initiatives such as INTECO or general in Spain such as "Asociación de Internautas" They are not subscribed to CERTS, they do **not pay attention to any specialized web and only few ones knew of Security issues by newspapers**, magazines or general purposed internet sites. So although they have heard of anti-virus, Trojans, malware, phishing or concepts related, they have **only end-user knowledge**, not appropriate for getting into business no matter the smaller their company is.

There is a **sense of non-alignment between Board of Directors and IT departments** or administrators in terms of security initiatives. It seems as **Board of Directors takes security mainly in terms of company public image,** seeking certificates to take commercial advantage from competitors. But for IT administrators there is a real concern about security, but as they do not have the overall business picture, they might pay attention to minor issues, mostly related to technical related incidents – virus, intruders, failures – rather than those that might well compromise seriously the Business Continuity – legal or organizational issues, as for example.

Most staff interviewed admitted that, they would like to implement recommended changes but there is a general lack of resources to achieve those changes if they are not regarded as critical by managers.

As security is a non-visible subject when everything works well, **prevention is not regarded as a priority**.

This is not only related to security but as overall problem in companies, there is an overall lack of interest in preventive measures. However and thanks to current Spanish regulations, most of Physical safeguards were set into place, mostly related to fire prevention . Same as for staff care and health conditions.

As the four companies were located in CEEI premises, physical access or overall physical security were similar managed in all companies. Depending on own procedures, some companies added additional measures but as overall, the maturity level of this safeguard was quite dependable of the CEEI buildings characteristics. In this way, CEEI or any type of global housing of new companies should also provide a Physical Risk Analysis to every company willing to be hosted as a preventive measure. We noticed that, as overall, information about the site and private guards were available in the two buildings studied.

None of the companies had documented all the procedures required. As documentation takes time, there is a general lack of it in SMEs studied. Staff that should be in charge of this task are normally postponing it as it is not enough regarded of interest by managers.

Another interesting point is related to **Organizational Issues and policies,** with special regard to employees.

All the companies studied trust so much in their employees, as most of them have been in the company for long-term basis.

There is little control on the staff behavior and it is not so odd that users configure and take self-care of their own PC.

There is also a general lack of accounting or track of staff actions in servers or any other critical asset. It is also not so odd to **trust all the security of the company in only one person** as **no manager interviewed thought about the betrayal possibility.**

Another interesting point is Risk Management. Some companies do not play well their cards in this area.

When there is a risk, **they do not make a serious exercise of overweighting all the possibilities and the balance cost-benefit of the safeguard to be introduced**.

The appliance solution is always the best regarded and sometimes the only one considered.

Few took into consideration the Risk Transference option such as for example, Insurance although this is quite on fashion in Western Society culture of making business.

About our experience with companies, we found them – with the exception of Machine Point - not so proactive as we expected, though all the four devoted the time agreed with them previously. Number of IT administrators is critical in achieving in a proactive way Risk Analysis. It there is not a minimum number, Risk Analysis will be leave out or not fully maintain through years.

The best **lesson learned** by all the companies is that **Risk Analysis** is a **DUTY** before promoting any initiative or investment in security. They also have learned to identify their goals, priorities, business processes and critical assets. Finally, they have been taught into continuously Risk Analysis, by either on a time basis or at lest every time their business needs or goals change or there is a modification in the critical assets inventory.

All the company reported that thanks to this Pilot they have noted **risks never regarded before**, as for example, those related to lack of Separation of Duties, lack of documentation or any other related to best security practices in an Organization.

6. GENERAL FINDINGS

The risk Management methodology for SMEs is a simplification that allows the small and medium Enterprise discovering the general security situation in their organization easily and intuitively. Moreover, the methodology allows identifying which actions should be taken to efficiently improve the security situation.

The main negative aspect detected is that there is a sense of non-alignment between Board of Directors and IT departments in terms of security initiatives. Most staff interviewed admitted that they would like to implement recommended changes but there is a general lack of resources to achieve those changes if they are not regarded as critical by managers. It seems as Board of Directors takes security mainly in terms of company public image, and they don't pay attention to other issues that might compromise seriously the Business Continuity.

In addition, the SMEs general thinking about the risk profile identification questionnaire is that questions are extremely general and they don't provide enough information about the specific threats and risk of the organization.

So, generally speaking, IT administrators thought that it would help introducing information about potential threats and what-if scenarios together with likelihood measures in order to raise awareness among management.

When it comes to the subject of dealing with safeguards determination, we would like to notice that most of the SMEs have found some problems mapping the suggested safeguards with practical implementations and they demanded us information on costless solutions to implement safeguards regarded by ENISA methodology. To our understanding, more practical explanations would be a great help for them in order to implement the safeguards.

By the way, the gap analysis process is an important but complicated step for the SMEs, to suggest a target implantation level for the safeguards could be a good approach to make it easier. The five level approach used in the report to identify the present and target implementation level for safeguards has been proved to be easy and understandable enough in order to allow the SMEs doing it by themselves.

Nevertheless, every SME participating in the pilot think that ENISA approach is good enough for them and it has motivated them to apply the risk management process in their day-to-day work. Moreover, most of the SMEs participating in the pilot admit to have increased their knowledge in themselves, especially about their critical assets, its security requirements and what they can do to protect those assets.

7. FEEDBACK FROM COMPANIES

To facilitate companies the feedback report through the Pilot, as well as a final interview at the time of report presentation with comments from personnel designed, a questionnaire was issued to companies with time enough to answer after the report was read.

Companies can test and experience with Pilar Tool its own report in the format used by the tool which was also issued to them inside a CD together with the temporal license as agreed in the Preliminary Workshop.

Here it is provided the average from companies and translated into English

Answers range from 1 – Nothing at all to 5 – Satisfactory

REPORT EVALUATION	4
Is the report generated easy to read and to understand?	3,75
Is the report comprehensive enough?	4
Does the report Provides new information about risk management and assessment?	3,5
Do you think the recommended controls and countermeasures are suitable?	4
Are you going to implement at least one of the recommended controls in the future?	4
GMV INTERVIEW EVALUATION	**4**
Do you think it has been easy to deal with GMV?	4,25
Has GMV been able to understand the security requirements of your company?	4
Has GMV provided to your company a new point of view about security?	3,75
Has GMV provided to your company “new knowledge” about risk management and assessment?	4,25
Do you consider that GMV has spent enough time?	4
WORKSHOP EVALUATION	**4**
Was the meeting arranged with sufficient prior notice?	4
Were the contents of the presentations of your interest?	3,5
Do you consider the time spent in the Workshop has been enough?	4
Has the Workshop showed the most important objectives of the project?	5
Has the Workshop satisfied your expectations?	3

ENISA RISK ASSESSMENT APPROACH EVALUATION	3,75
Is the ENISA risk assessment approach clearly defined in the report generated?	3,33
Do you think that such approach consider the most relevant aspects of your organization?	4,75
Would you like to know more about risk assessment or the ENISA approach?	3,33
Is your organization more motivated now than before your participation in this Project to make progress in security information management aspects?	4,33
Do you feel comfortable with ENISA risk assessment approach?	3,33
PILAR SOFTWARE EVALUATION	**3**
Do you think PILAR is useful in the risk assessment process?	3
Do you think PILAR is easy to use?	2,5
Do you find useful the kind of reports generated by PILAR?	3
Do you understand every risk assessment concept used by PILAR?	3,5
Are you going to use PILAR in the future?	3,75

As a result of this questionnaire and with comments made by the final interview and the Final Workshop there come some conclusions:

1.- **Report generated with the Risk Analysis per company and time devoted by GMV to every company is very good in general**, although we feel we could have extend a little bit more about Risk Analysis and Risk Management process in overall, as it is the start point to understand any methodology suggested. Another point of interest is the language used. Though we have added an executive summary readable for the Board of Directors, we have the sense that they wanted more graphics, and more "**what if"** scenarios to give Board of Directors ideas on the consequences of the incidents that might arise because of the threats due to lack of safeguards.

2.- **Preliminary Workshop and Final Workshop,** although they were quite interesting for those companies present, they have not reach enough quorum because more than half of the companies did not attend despite they were recall with time enough.

3.- **ENISA approach is good enough for companies**, however some clarifications, improvements and introduction will be highly desirable for companies to understand what is all about.

4.- **PILAR basic Tool used for Risk Management and Report generation is also good enough for companies**, however it must be improved to facilitate SMEs a better installation and use. Most of the users in SMEs that are likely to go on using this tool admit they will not be capable of making a new report from scratch but only to maintain the file provided by GMV.

5.- **PILAR tool succeeds in terms of Risk Management understanding**. It contains a very nice help menu that explains fairly well every concept related to Risk Management.

8. REFERENCES

Below it is referenced the documents and references that have been used to deal with the new ENISA Risk Assessment Methodology within this PILOT.

Code	Name of the Document
[ENISA-INF]	Information Package for SMEs
[ENISA-RM&IT]	Risk Management & IT Security for Micro and Small Businesses
[ENISA-WWW]	*http://www.enisa.europa.eu*
[MAGERITV2]	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
[BIOM-WWW]	*http://www.institutobiomar.com*
[MACH-WWW]	*http://machinepoint.com*
[PROX-WWW]	*http://www.proximasystems.net*
[BESEL-WWW]	*http://www.besel.es*
[ASINT-WWW]	*http://www.internautas.org*

APPENDIX I – INITIAL QUESTIONNAIRE ISSUED TO COMPANIES

The questionnaires have been written in Spanish, the language used by the companies. They have included several chapters in order to gather information pertinent to the profile selection and safeguard levels.

ACTIONS ON IT SECURITY (ACTUACIONES DE SEGURIDAD DE LA INFORMACIÓN)

Conteste brevemente a las siguientes preguntas:
1. ¿Está su empresa organizada en diferentes secciones dirigidas por diferentes responsables o existe un único jefe para todo el personal?
2. ¿Dispone de conocimientos técnicos especializados en sistemas y redes de TI?
3. ¿Cuenta con recursos humanos con conocimientos de TI y disponibles?
4. ¿Dependen sus actividades poco de los sistemas de TI y no implican el almacenamiento o proceso de datos sobre sus clientes de índole sensible (datos personales, historial clínico, …)? ¿Ha participado su organización en actividades similares, como las relativas a procesos de mejora de la calidad?
5. ¿Puede disponer de un grupo de tres a cinco personas que cuenten con un conocimiento amplio y profundo de la organización y posean además la mayor parte de las destrezas que siguen? ▪ capacidad para la resolución de problemas ▪ capacidad analítica ▪ capacidad para trabajar en equipo ▪ destrezas de liderazgo ▪ capacidad para comprender los procesos empresariales de la compañía y la infraestructura subyacente a la organización ▪ capacidad para pasar unos días trabajando en este **método.**
6. ¿Dispone de una infraestructura de tecnología de la información relativamente sencilla que sea bien conocida al menos por un miembro de su organización?
7. ¿Considera necesario prestar especial atención a las competencias esenciales y los procesos empresariales estratégicos?

8. ¿Implican sus actividades empresariales y sus ofertas de servicios transacciones financieras (comercio electrónico, etc.)?
9. ¿Está su empresa sujeta en gran medida a unos requisitos o una legislación nacional o comunitaria rigurosos?
10. ¿Considera necesario seguir haciendo hincapié en las competencias esenciales y los procesos empresariales estratégicos, pero también mejorar el grado de sensibilización interno respecto a la seguridad de la información y la competencia en asuntos que atañen a ésta?
11. ¿Cuenta con una infraestructura de TI compleja y relativamente grande, pero con un modelo de negocio relativamente simple?

RISK PROFILE (PERFIL DE RIESGO)

Para cada una de las áreas de riesgo marque la opción que mejor se adapte a su empresa. Marca una única respuesta con un ☒	
1.	**Riesgos jurídicos**
☐	La organización maneja información relativa a los clientes de carácter sensible y personal, incluidas historias médicas y datos personales críticos, con arreglo a lo previsto en la legislación de protección de datos de la UE.
☐	La organización maneja información de los clientes de carácter personal, pero no sensible, con arreglo a lo dispuesto en la legislación de protección de datos de la UE.
☐	La organización no maneja datos personales distintos a los del personal empleado.
2.	**Riesgos de productividad**
☐	La organización emplea a más de 100 personas que requieren a diario del acceso a aplicaciones y servicios empresariales.
☐	La organización emplea a más de 50 personas que requieren a diario del acceso a aplicaciones y servicios empresariales.
☐	La organización emplea a menos de 10 personas que requieren a diario del acceso a aplicaciones y servicios empresariales.
3.	**Riesgos para la estabilidad financiera**
☐	Los ingresos anuales de la organización exceden de 25 millones de euros y/o se producen transacciones financieras con terceros o clientes como proceso habitual dentro de la actividad empresarial.
☐	Los ingresos anuales de la organización no exceden de 25 millones de euros.
☐	Los ingresos anuales de la organización no exceden de 5 millones de euros.

4. Riesgos para la reputación y de pérdida de confianza de los clientes	
☐	La indisponibilidad o la calidad del servicio repercuten directamente en la actividad de la organización, y/o más del 70% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa.
☐	La indisponibilidad o la calidad del servicio pueden repercutir indirectamente en la actividad de la organización, y/o menos del 5% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa.
☐	La indisponibilidad o la calidad del servicio no pueden repercutir de manera directa o indirecta en la actividad de la organización, ni derivar en pérdida de ingresos.

SECURITY PRACTICES (PRÁCTICAS DE SEGURIDAD)

Infraestructura
1. ¿Dispone su empresa de servicios accesibles online?
2. ¿Dónde se encuentran los servicios accesibles online de la empresa?¿servidores ubicados en las instalaciones, empresas externas de hosting/housing, ...?
3. ¿Dispone su empresa de un servidor de correo dedicado o es un servicio externalizado?
4. ¿Los servidores de su empresa se encuentran en una ubicación dedicada (CPD, habitación independiente) o compartida con otras empresas o los puestos de usuario?
5. ¿Cuántas personas tienen acceso a dichos equipos?
6. ¿Se planifican las actuaciones a realizar en los equipos?
7. ¿Se realiza un mantenimiento y actualización software de los sistemas?
8. ¿Se dispone de esquemas actualizados de los sistemas y la infraestructura de red?
9. ¿Se controla el tráfico de red mediante el uso de dispositivos firewall?

Control Antivirus
1. ¿Dispone de algún mecanismo de control antispam?
2. ¿Disponen los equipos de trabajo de software antivirus actualizado?
3. ¿Tienen los empleados de la empresa acceso a Internet?
4. ¿Se restringe de alguna manera las páginas de Internet accedidas por los empleados?

Control de Acceso Lógico
1. ¿Se aplican controles de acceso y mecanismos de autenticación apropiados como por ejemplo Directorio Activo?
2. ¿Tienen los empleados permisos de administrador sobre los equipos?
3. ¿Tienen los empleados permisos para instalar software en sus equipos?
4. ¿Se realiza un cambio periódico de las contraseñas de acceso a los sistemas?¿Se fuerza este cambio de forma automática?
5. ¿Los puestos de trabajo son personales o compartidos?
6. ¿Se permite en la empresa el teletrabajo?
7. ¿Existen equipos en la empresa que salgan habitualmente de las instalaciones? (portátiles)

Política de Personal y Formación
1. ¿Se realiza algún tipo de comprobación antes de la incorporación de nuevo personal? (verificación de referencias, formación, etc.)
2. ¿Esta procedimentado el alta y baja de empleados en los sistemas?

3. ¿Reciben las nuevas incorporaciones algún tipo de formación sobre las prácticas de seguridad de la empresa?

Estrategia de Seguridad

1. ¿Está la empresa concienciada con la seguridad y se traslada dicha preocupación a los empleados de alguna manera?
2. ¿Existe un presupuesto fijo asignado a los aspectos relacionados con la seguridad de la información o a mantenimiento de sistemas de IT?
3. ¿Existen procedimientos documentados en materia de seguridad?

Soportes de información

1. ¿Cómo se realizan en su empresa las reuniones de trabajo habitualmente? (puesto de trabajo, salas compartidas con otras empresas, etc.)
2. ¿Se permite el uso de medios de almacenamiento removibles? (pendrive)
3. ¿El almacenamiento de ficheros y trabajo diario se realiza sobre un servidor de ficheros centralizado o en los propios equipos de usuario?
4. ¿Se realizan de forma periódica copias de la información relevante?¿Está automatizada dicha operación de backup?
5. ¿Se realizan verificaciones periódicas de las copias de backup realizadas?
6. ¿Dónde se almacenan las copias de backup realizadas?

Desarrollo de software

1. ¿Se realizan en su empresa tareas de desarrollo de software?

2. ¿Se hace uso de algún tipo de software de control de versiones?
3. ¿Se realizan copias diarias del código fuente?

Seguridad física
1. ¿Su empresa se encuentra ubicada en un edificio propio o compartido?
2. ¿Se debe atravesar algún control de acceso para acceder a las instalaciones de la empresa?¿cual? (recepción, puerta cerrada con llave, tarjeta identificativa, ...)
3. ¿Se controlan y registran de alguna manera los accesos al edificio en el que se ubica su empresa de alguna manera?
4. ¿Maneja su empresa materiales peligrosos que impliquen riesgos de incendio, explosión, contaminación química, ...?
5. ¿Existen en las proximidades empresas que manejen materiales peligrosos que impliquen riesgos de incendio, explosión, contaminación química, ...?

APPENDIX II – FINAL QUESTIONNAIRE ISSUED TO COMPANIES FOR FEEDBACK REPORTING.

Responda a las siguientes preguntas valorando del 1-Poco al 5-Mucho
VALORACIÓN DEL INFORME ENTREGADO
1. ¿Les parece comprensible el informe?
2. ¿Les parece suficientemente completo?
3. ¿Les da información sobre riesgos que no habían considerado?
4. ¿Les parecen adecuadas las salvaguardas?
5. ¿Piensan implementar en un futuro próximo alguna o varias de las salvaguardas propuestas?
VALORACIÓN DE LA ENTREVISTA CON GMV
1. ¿Les ha parecido fácil la comunicación y el trato con esta empresa?
2. ¿Ha sabido GMV captar sus necesidades e inquietudes en el ámbito de la seguridad?
3. ¿Les ha proporcionado una nueva visión sobre la seguridad?
4. ¿Les ha aportado conocimientos nuevos sobre el análisis de riesgos?
5. ¿Les ha parecido el tiempo dedicado por GMV suficiente?

Responda a las siguientes preguntas valorando del 1-Poco al 5-Mucho
VALORACIÓN DEL WORKSHOP INICIAL (si pudo asistir)
1. ¿Les informaron con tiempo suficiente?
2. ¿Les han resultado de interés las presentaciones?
3. ¿Les ha parecido suficiente la duración del Workshop?
4. ¿Les ha proporcionado una idea clara de los objetivos del piloto?
5. ¿Ha satisfecho sus expectativas iniciales?
VALORACIÓN DE LA METODOLOGÍA ENISA
1. ¿A través del informe comprenden de forma clara la metodología seguida por ENISA?
2. ¿Creen que dicha metodología contempla todos los elementos de interés de su organización?
3. ¿Les gustaría tener más información sobre esta metodología o sobre el análisis de riesgos en general?
4. ¿Les ha animado el piloto a progresar en materia de seguridad con nuevas acciones como por ejemplo realizar auditorías, implantar sistemas de gestión de la seguridad, etc.?
5. ¿Se sienten cómodos con la metodología empleada?

Responda a las siguientes preguntas valorando del 1-Poco al 5-Mucho
VALORACIÓN DE LA HERRAMIENTA PILAR
1. ¿Les ha parecido claro su uso dentro del análisis de riesgos?
2. ¿Les ha parecido fácil de usar?
3. ¿Les parece interesante el formato de informes que presenta?
4. ¿Entienden todos los conceptos que emplea la herramienta?
5. ¿Piensa seguir utilizándola para mantener actualizado su informe?
OTROS COMENTARIOS
Indique aquí cualquier otro comentario que considere de interés que no esté recogido en los apartados anteriores o que quiera completar

APPENDIX III – RESPONSES FROM COMPANIES

PROXIMA S.L.

(MICRO SME)

Responda a las siguientes preguntas valorando del 1-Poco al 5-Mucho	
VALORACIÓN DEL INFORME ENTREGADO	
1.	**¿Les parece comprensible el informe?**
4	
2.	**¿Les parece suficientemente completo?**
5	
3.	**¿Les da información sobre riesgos que no habían considerado?**
4	
4.	**¿Les parecen adecuadas las salvaguardas?**
4	
5.	**¿Piensan implementar en un futuro próximo alguna o varias de las salvaguardas propuestas?**
5	
VALORACIÓN DE LA ENTREVISTA CON GMV	
1.	**¿Les ha parecido fácil la comunicación y el trato con esta empresa?**
4	
2.	**¿Ha sabido GMV captar sus necesidades e inquietudes en el ámbito de la seguridad?**
4	
3.	**¿Les ha proporcionado una nueva visión sobre la seguridad?**
3	
4.	**¿Les ha aportado conocimientos nuevos sobre el análisis de riesgos?**
4	
5.	**¿Les ha parecido el tiempo dedicado por GMV suficiente?**
4	

Responda a las siguientes preguntas valorando del 1-Poco al 5-Mucho
VALORACIÓN DEL WORKSHOP INICIAL (si pudo asistir)
1. ¿Les informaron con tiempo suficiente?
4
2. ¿Les han resultado de interés las presentaciones?
3
3. ¿Les ha parecido suficiente la duración del Workshop?
4
4. ¿Les ha proporcionado una idea clara de los objetivos del piloto?
5
5. ¿Ha satisfecho sus expectativas iniciales?
4
VALORACIÓN DE LA METODOLOGÍA ENISA
1. ¿A través del informe comprenden de forma clara la metodología seguida por ENISA?
4
2. ¿Creen que dicha metodología contempla todos los elementos de interés de su organización?
4
3. ¿Les gustaría tener más información sobre esta metodología o sobre el análisis de riesgos en general?
3
4. ¿Les ha animado el piloto a progresar en materia de seguridad con nuevas acciones como por ejemplo realizar auditorías, implantar sistemas de gestión de la seguridad, etc.?
5
5. ¿Se sienten cómodos con la metodología empleada?
4

Responda a las siguientes preguntas valorando del 1-Poco al 5-Mucho
VALORACIÓN DE LA HERRAMIENTA PILAR
1. ¿Les ha parecido claro su uso dentro del análisis de riesgos?
3
2. ¿Les ha parecido fácil de usar?
3
3. ¿Les parece interesante el formato de informes que presenta?
4
4. ¿Entienden todos los conceptos que emplea la herramienta?
3
5. ¿Piensa seguir utilizándola para mantener actualizado su informe?
3
OTROS COMENTARIOS
Indique aquí cualquier otro comentario que considere de interés que no esté recogido en los apartados anteriores o que quiera completar

MACHINE POINT S.L.

(The most proactive SME in the Pilot)

Responda a las siguientes preguntas valorando del 1-Poco al 5-Mucho	
VALORACIÓN DEL INFORME ENTREGADO	
1.	**¿Les parece comprensible el informe?**
4	
2.	**¿Les parece suficientemente completo?**
4	
3.	**¿Les da información sobre riesgos que no habían considerado?**
4	
4.	**¿Les parecen adecuadas las salvaguardas?**
3	
5.	**¿Piensan implementar en un futuro próximo alguna o varias de las salvaguardas propuestas?**
4	
VALORACIÓN DE LA ENTREVISTA CON GMV	
1.	**¿Les ha parecido fácil la comunicación y el trato con esta empresa?**
4	
2.	**¿Ha sabido GMV captar sus necesidades e inquietudes en el ámbito de la seguridad?**
4	
3.	**¿Les ha proporcionado una nueva visión sobre la seguridad?**
4	
4.	**¿Les ha aportado conocimientos nuevos sobre el análisis de riesgos?**
5	
5.	**¿Les ha parecido el tiempo dedicado por GMV suficiente?**
3	

Responda a las siguientes preguntas valorando del 1-Poco al 5-Mucho
VALORACIÓN DEL WORKSHOP INICIAL (si pudo asistir)
1. ¿Les informaron con tiempo suficiente?
4
2. ¿Les han resultado de interés las presentaciones?
4
3. ¿Les ha parecido suficiente la duración del Workshop?
4
4. ¿Les ha proporcionado una idea clara de los objetivos del piloto?
5
5. ¿Ha satisfecho sus expectativas iniciales?
2 (en principio pensabamos que este proyecto era una auditoria de seguridad)
VALORACIÓN DE LA METODOLOGÍA ENISA
1. ¿A través del informe comprenden de forma clara la metodología seguida por ENISA?
2
2. ¿Creen que dicha metodología contempla todos los elementos de interés de su organización?
5
3. ¿Les gustaría tener más información sobre esta metodología o sobre el análisis de riesgos en general?
3
4. ¿Les ha animado el piloto a progresar en materia de seguridad con nuevas acciones como por ejemplo realizar auditorías, implantar sistemas de gestión de la seguridad, etc.?
4
5. ¿Se sienten cómodos con la metodología empleada?
2

Responda a las siguientes preguntas valorando del 1-Poco al 5-Mucho	
VALORACIÓN DE LA HERRAMIENTA PILAR	
1.	**¿Les ha parecido claro su uso dentro del análisis de riesgos?**
3	
2.	**¿Les ha parecido fácil de usar?**
1	
3.	**¿Les parece interesante el formato de informes que presenta?**
2	
4.	**¿Entienden todos los conceptos que emplea la herramienta?**
2	
5.	**¿Piensa seguir utilizándola para mantener actualizado su informe?**
2	
OTROS COMENTARIOS	
Indique aquí cualquier otro comentario que considere de interés que no esté recogido en los apartados anteriores o que quiera completar	

INSTITUTO BIOMAR S.A.

Responda a las siguientes preguntas valorando del 1-Poco al 5-Mucho	
VALORACIÓN DEL INFORME ENTREGADO	
1.	**¿Les parece comprensible el informe?**
4	
2.	**¿Les parece suficientemente completo?**
4	
3.	**¿Les da información sobre riesgos que no habían considerado?**
4	
4.	**¿Les parecen adecuadas las salvaguardas?**
5	
5.	**¿Piensan implementar en un futuro próximo alguna o varias de las salvaguardas propuestas?**
4	

VALORACIÓN DE LA ENTREVISTA CON GMV	
1.	**¿Les ha parecido fácil la comunicación y el trato con esta empresa?**
5	
2.	**¿Ha sabido GMV captar sus necesidades e inquietudes en el ámbito de la seguridad?**
4	
3.	**¿Les ha proporcionado una nueva visión sobre la seguridad?**
5	
4.	**¿Les ha aportado conocimientos nuevos sobre el análisis de riesgos?**
5	
5.	**¿Les ha parecido el tiempo dedicado por GMV suficiente?**
5	

Responda a las siguientes preguntas valorando del 1-Poco al 5-Mucho
VALORACIÓN DEL WORKSHOP INICIAL (si pudo asistir)
1. ¿Les informaron con tiempo suficiente?
2. ¿Les han resultado de interés las presentaciones?
3. ¿Les ha parecido suficiente la duración del Workshop?
4. ¿Les ha proporcionado una idea clara de los objetivos del piloto?
5. ¿Ha satisfecho sus expectativas iniciales?
VALORACIÓN DE LA METODOLOGÍA ENISA
1. ¿A través del informe comprenden de forma clara la metodología seguida por ENISA?
4
2. ¿Creen que dicha metodología contempla todos los elementos de interés de su organización?
5
3. ¿Les gustaría tener más información sobre esta metodología o sobre el análisis de riesgos en general?
4
4. ¿Les ha animado el piloto a progresar en materia de seguridad con nuevas acciones como por ejemplo realizar auditorías, implantar sistemas de gestión de la seguridad, etc.?
4
5. ¿Se sienten cómodos con la metodología empleada?
4

Responda a las siguientes preguntas valorando del 1-Poco al 5-Mucho	
VALORACIÓN DE LA HERRAMIENTA PILAR	
1.	**¿Les ha parecido claro su uso dentro del análisis de riesgos?**
4	
2.	**¿Les ha parecido fácil de usar?**
4	
3.	**¿Les parece interesante el formato de informes que presenta?**
4	
4.	**¿Entienden todos los conceptos que emplea la herramienta?**
4	
5.	**¿Piensa seguir utilizándola para mantener actualizado su informe?**
5	
OTROS COMENTARIOS	
Indique aquí cualquier otro comentario que considere de interés que no esté recogido en los apartados anteriores o que quiera completar	
5 LA PROFESIONALIDAD Y AMABILIDAD DEL PERSONAL, TANTO DE LA SRTA. MARIA TERESA AVELINO COMO DEL SR. JAIRO MONTERO	

BESEL S.A.

(The less proactive to the pilot among the four).

Responda a las siguientes preguntas valorando del 1-Poco al 5-Mucho	
VALORACIÓN DEL INFORME ENTREGADO	
1.	**¿Les parece comprensible el informe?**
3	
2.	**¿Les parece suficientemente completo?**
3	
3.	**¿Les da información sobre riesgos que no habían considerado?**
2	
4.	**¿Les parecen adecuadas las salvaguardas?**
4	

5.	¿Piensan implementar en un futuro próximo alguna o varias de las salvaguardas propuestas?
3	

VALORACIÓN DE LA ENTREVISTA CON GMV	
1.	¿Les ha parecido fácil la comunicación y el trato con esta empresa?
4	
2.	¿Ha sabido GMV captar sus necesidades e inquietudes en el ámbito de la seguridad?
4	
3.	¿Les ha proporcionado una nueva visión sobre la seguridad?
3	
4.	¿Les ha aportado conocimientos nuevos sobre el análisis de riesgos?
3	
5.	¿Les ha parecido el tiempo dedicado por GMV suficiente?
4	

Responda a las siguientes preguntas valorando del 1-Poco al 5-Mucho
VALORACIÓN DEL WORKSHOP INICIAL (si pudo asistir)
1. ¿Les informaron con tiempo suficiente?
2. ¿Les han resultado de interés las presentaciones?
3. ¿Les ha parecido suficiente la duración del workshop?
4. ¿Les ha proporcionado una idea clara de los objetivos del piloto?
5. ¿Ha satisfecho sus expectativas iniciales?
VALORACIÓN DE LA METODOLOGÍA ENISA
1. ¿A través del informe comprenden de forma clara la metodología seguida por ENISA?
2. ¿Creen que dicha metodología contempla todos los elementos de interés de su organización?
3. ¿Les gustaría tener más información sobre esta metodología o sobre el análisis de riesgos en general?
4. ¿Les ha animado el piloto a progresar en materia de seguridad con nuevas acciones como por ejemplo realizar auditorías, implantar sistemas de gestión de la seguridad, etc.?
5. ¿Se sienten cómodos con la metodología empleada?

Responda a las siguientes preguntas valorando del 1-Poco al 5-Mucho	
VALORACIÓN DE LA HERRAMIENTA PILAR	
1.	**¿Les ha parecido claro su uso dentro del análisis de riesgos?**
2	
2.	**¿Les ha parecido fácil de usar?**
2	
3.	**¿Les parece interesante el formato de informes que presenta?**
2	
4.	**¿Entienden todos los conceptos que emplea la herramienta?**
5	
5.	**¿Piensa seguir utilizándola para mantener actualizado su informe?**
5	
OTROS COMENTARIOS	
Indique aquí cualquier otro comentario que considere de interés que no esté recogido en los apartados anteriores o que quiera completar	

ANNEX : SANITIZED RISK ANALYSIS REPORTS

To guarantee the anonymity of every company involved we are not providing information such as name, accurate assets, specific vulnerabilities encountered, activity or any other information that can lead to a easy guessing of the company the report is about.

In addition, we have set the date and codes of the documents provided to default dates and codes not to give an idea of who are who because of the order, date or number.

We have given random names A, B, C and D to companies.

Informe de Análisis de Riesgos 30.09.2008

(SME A)

Preparado:	GMV Soluciones Globales Internet	Clasification Type After Sanitization:	UNCLASSIFIED
Verificado:	N/A	Código:	SGI-ERNSTING-INF-xxx
Aprobado:	Mª Teresa Avelino Carmona	Versión:	1
Autorizado:	Mª Teresa Avelino Carmona	Fecha:	30/09/2008

GMV SOLUCIONES GLOBALES INTERNET S.A.
P.T. Boecillo Parcela 101 - 47151 Valladolid.
Tel.: +34 983 54 65 54, Fax: +34 983 54 65 53.
www.gmv-sgi.es, www.gmv.com.

Código Interno: SGISA xxx/08

ESTA PÁGINA SE HA DEJADO EN BLANCO INTENCIONADAMENTE.

HOJA DE ESTADO DEL DOCUMENTO

Versión	Fecha	Págs.	Procesador	Cambios
1	30/09/2008	39	Word 2000 español	Primera versión

ÍNDICE

LISTA DE TABLAS Y FIGURAS

1. INTRODUCCIÓN

1.1. PROPÓSITO

El objeto del presente documento es plasmar los resultados obtenidos tras el análisis de riesgos realizado sobre los activos de información e instalaciones englobados en el alcance del mismo. Este análisis de riesgos se ha realizado dentro del ámbito de desarrollo del piloto de ENISA para la aplicación de su metodología adaptada a PYMES de análisis de riesgos, haciendo uso de la herramienta Pilar Basic 4.3 como apoyo para la aplicación de dicha metodología.

1.2. ALCANCE

El alcance del presente documento abarca las instalaciones y activos de información relativos a la actividad desarrollada en la sede de empresa A ubicada en X[1]

1.3. DEFINICIONES Y ACRÓNIMOS

1.3.1. DEFINICIONES

Concepto	Definición
Activo	Elementos del sistema de información que aportan valor a la organización
Confidencialidad	Garantía de que la información es accesible sólo a aquellas personas autorizadas a tener acceso a ella.
Disponibilidad	Garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.
Integridad	Garantía de que se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
Autenticación	Identificación de quién hace uso de los datos o servicios
Amenaza	Sucesos que pueden materializarse causando un perjuicio a la organización
Vulnerabilidad	Posibilidad de materialización de una amenaza sobre un activo
Riesgo	Índice que integra la probabilidad de que un escenario se materialice y la degradación que supondría sobre un activo
Impacto	Índice de daño o presión al que se ve sometido un servicio, proceso o activo en caso de la materialización de una amenaza
Salvaguardas	Elementos de defensa desplegados para reducir el perjuicio para la organización en caso de materialización de una amenaza

1.3.2. ACRÓNIMOS

Acrónimo	Concepto
[D]	Disponibilidad
[I]	Integridad
[C]	Confidencialidad
UE	Unión Europea

[1] SME name and location

2. REFERENCIAS

Los siguientes documentos son aplicables en la medida que tengan carácter contractual o hayan sido aprobados por el cliente, correspondiéndose sus versiones y fechas con las vigentes en el momento de publicación del presente documento; el resto se han usado simplemente a modo de soporte.

Código	Documento
[ENISA-INF]	Paquete informativo para PYME
[MAGERITV2]	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

3. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS[2]

Hoy en día nos encontramos en un entorno en el que la información se ha convertido en uno de los principales activos de cualquier organización. Se debe entender información en un sentido amplio, independientemente de la forma en la que se guarde o se transmita. Por lo tanto, esta información debe gestionarse y protegerse estratégicamente y de forma proactiva, incluyendo los sistemas y equipos o recursos que contribuyen a su almacenamiento, proceso y transmisión.

La gestión y protección de la información crítica de la organización deber realizarse de forma inteligente, identificando los procesos de negocio, los componentes que sustentan dichos procesos y las amenazas potenciales que podrían poner en peligro la normal ejecución de los mismos. Este esfuerzo de identificación y análisis debe facilitar la toma de decisiones en cuestión de seguridad, permitiendo priorizar las actuaciones que deben realizarse y optimizar el uso de los recursos. Esta tarea de análisis para la identificación de los puntos críticos de negocio y de las principales amenazas es una práctica que debe aplicarse de forma global y sistemática en el transcurso de la actividad diaria de la organización con el fin de invertir en seguridad de una forma racional, protegiendo aquellos activos que lo necesitan y con la intensidad necesaria.

Es aquí donde entra en juego el análisis de riesgos, que pretende sistematizar todo este proceso de análisis e identificación de actividades críticas para el negocio y amenazas potenciales con el fin de estimar la magnitud de los riesgos a los que está expuesta una organización. Esto permitirá conocer el estado actual de la organización en materia de seguridad, de forma que se pueda realizar una gestión adecuada de los riesgos identificados. Esta gestión de los riesgos consistirá en la planificación e implantación de las salvaguardas adecuadas de acuerdo a los objetivos, política y estrategia de la organización con el fin de reducir, transferir o asumir dichos riesgos. El riesgo no se puede erradicará totalmente, sino que el objetivo será reducirle a un nivel residual que sea asumible para la organización.

De forma general se puede dividir el proceso de análisis de riesgos en cuatro fases diferenciadas:

1. Identificación de activos relevantes para la organización. Entendiendo activo como cualquier recurso de información o relacionado con ésta necesario para la correcta ejecución de la actividad de la organización. Es obvio que no todos los activos son iguales, sino que pertenecerán a diferentes categorías (red, hardware, software, personas, etc.), lo cual condicionará las potenciales amenazas y las salvaguardas aplicables.
2. Identificación de amenazas. Amenazas son todos aquellos sucesos que pueden ocurrir y que puede causar un perjuicio a la organización. No todas las amenazas afectan a todos los activos, sino que hay una dependencia directa entre el tipo de activo y lo que le podría ocurrir. Así, podrían extorsionar a un empleado de la organización, mientras que no ocurre lo mismo con una aplicación o un servidor. De igual forma, no todos los activos se ven afectados de igual manera ni en el mismo grado por una determinada amenaza, por lo tanto es importante estimar cómo de vulnerable es un determinado activo atendiendo a dos aspectos:
    - Degradación: Cómo de perjudicado se vería el activo ante la materialización de la amenaza. Suele expresarse como un porcentaje del valor del activo.
    - Frecuencia: Cada cuanto es probable que se materialice la amenaza. Proporciona una nueva dimensión a la degradación que puede causar una amenaza, ya que una amenaza puede ser de terribles consecuencias pero de muy probable

[2] Here comes a short description about risk analysis process for an easier understanding of the report and the concepts used on it. a short explanation about the ENISA approach is also included in this section

materialización otra podría ser de muy bajas consecuencias pero tan frecuente como para acabar acumulando un daño considerable.

Mientras que estos dos aspectos nos determinan la forma en que una amenaza puede afectar un activo, es necesario determinar en qué sentido se puede producir este perjuicio. Para ello se pueden considerar tres dimensiones en las que un activo de información podría verse afectado:

- Disponibilidad: Se debe evaluar el perjuicio de que el activo no esté o no pueda ser utilizado.
- Confidencialidad: Se debe evaluar el perjuicio de que la información sea conocida por quien no debe.
- Integridad: Se debe valorar el perjuicio de que el activo o la información pueda estar manipulada, dañada o corrupta.

3. Identificación de salvaguardas existentes. Hasta este punto no se han tenido en cuenta las salvaguardas desplegadas, se tiene por lo tanto un mapa del riesgo potencial de la organización en el que se determinan los impactos y riesgos a que estarían expuestos los activos si no se protegieran, lo cual no es habitual. Las salvaguardas pueden tener dos efectos en el riesgo presente, bien reduciendo la frecuencia o la probabilidad de que una amenaza se materialice (salvaguardas preventivas) o bien limitando el impacto producido por una amenaza. Se puede considerar una salvaguarda efectiva al 100% cuando:

   - Es teóricamente idónea
   - Está perfectamente desplegada, configurada y mantenida
   - Se emplea siempre
   - Existen procedimientos claros de uso normal y en caso de incidencias
   - Los usuarios están formados y concienciados
   - Existen controles que avisan de posibles fallos

La forma en que se relacionan todos estos elementos se muestra en la siguiente figura:

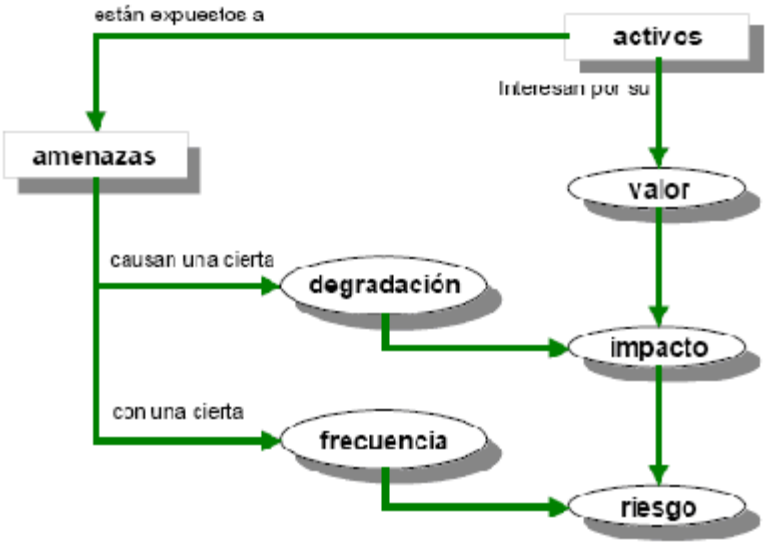

Figura 1: Relación de conceptos en el mapa de riesgos potencial

Una vez finalizado el análisis de riesgos se debe haber obtenido una visión de los impactos y riesgos residuales de la organización con las salvaguardas existentes. En el caso de que el riesgo residual no sea despreciable o asumible por la organización se tendrán que planificar y adoptar medidas que permitan alcanzar ese nivel de riesgo asumible para la organización. Es esto lo que se entiende por Gestión del Riesgo.

Durante el proceso de gestión del riesgo se deben seleccionar de forma prioritaria aquellas salvaguardas de tipo preventivo que permitan minimizar la probabilidad de que las amenazas se materialicen o que el daño producido sea despreciable. No obstante, dado que esto no es siempre posible, se deben adoptar en cualquier caso las medidas necesarias para que un posible incidente de seguridad no pase inadvertido, permitiendo su pronta detección, una reacción adecuada mediante un plan de emergencia y la posibilidad de recuperar el sistema a sus condiciones aceptables de funcionamiento lo antes posible mediante la elaboración de planes de continuidad.

Por último, debe tenerse en cuenta que una aplicación de salvaguardas eficiente debe llegar a un cierto equilibrio entre:

- Salvaguardas técnicas: en aplicaciones, equipos y comunicaciones
- Salvaguardas físicas: protegiendo el entorno de trabajo de las personas y los equipos
- Medidas de organización: de prevención y gestión de las incidencias
- Política de personal: siendo el factor humano el eslabón más débil de la seguridad, resulta de vital importancia contar con medidas adecuadas de contratación de personal, formación continua en buenas prácticas de seguridad, fomentar la participación en el reporte de incidencias y la aplicación de medidas disciplinarias cuando las normativas y política se seguridad de la organización se ven quebrantadas.

En cualquier caso se debe tener siempre presente que el punto óptimo vendrá dado por el equilibrio entre el valor del activo a proteger y la inversión realizada en salvaguardas para

protegerlo, considerando el valor del activo no sólo por su valor económico sino también en términos estratégicos, de reputación, etc.

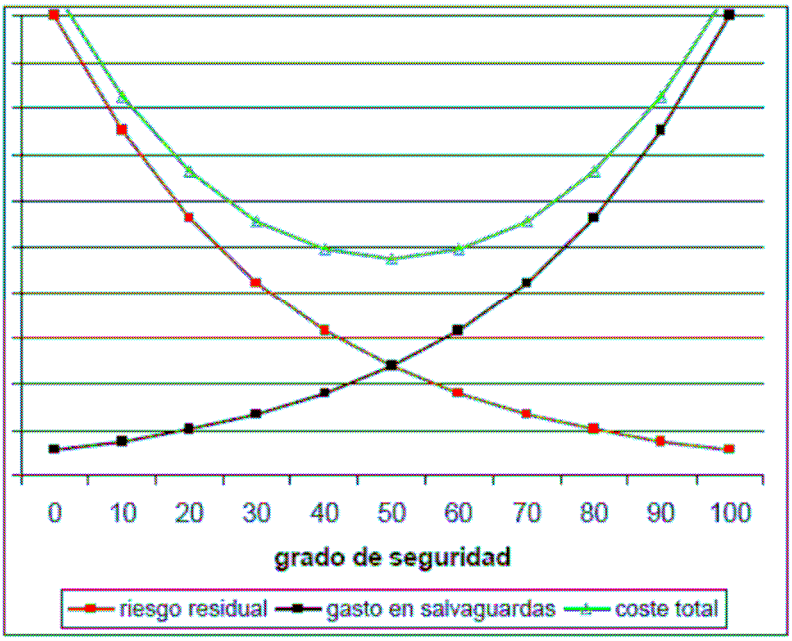

Figura 2: Grado de seguridad

En cuanto al proceso general de análisis de riesgos cabe destacar que existen diferentes metodologías que aportan diferentes enfoques a cada una de las diferentes fases que se pueden diferenciar, no obstante la mayor parte de ellas coinciden en la base conceptual y los objetivos, que han intentado plasmarse en el presente apartado.

El análisis de riesgos realizado dentro del ámbito de este piloto y cuyos resultados se expondrán en el presente documento se basa en la metodología desarrollada por ENISA. El principal objetivo de dicha metodología es la elaboración de un modelo simplificado de análisis de riesgos enfocado a pequeñas organizaciones que permita a dichas organizaciones realizar una evaluación del riesgo presente en sus entornos y seleccionar las medidas pertinentes para gestionar los riesgos identificados con un esfuerzo proporcional a sus recursos.

La metodología ENISA se basa en un enfoque en cuatro fases que tratan los siguientes aspectos:

1. Selección del perfil de riesgos: En esta fase se evalúa el perfil de riesgo de la organización mediante la utilización de un conjunto predefinido de criterios estructurados en una tabla de evaluación en la que la organización debe situarse.
2. Identificación de los activos críticos: En esta fase se seleccionan los activos más importantes en los procesos de negocio de la organización definiendo los requisitos de seguridad para cada uno de dichos activos y clasificándoles según su naturaleza.
3. Selección de tarjetas de controles o salvaguardas: Basándose en el perfil de riesgo de la organización y los requisitos de seguridad definidos para los activos de la empresa se seleccionan unos controles o salvaguardas aplicables.
4. Ejecución y gestión: Una vez determinados todos los aspectos anteriores y analizada la situación actual frente a la deseada se deben asignar prioridades en la ejecución de los controles.

Como herramienta de apoyo para aplicar la metodología se ha hecho uso de la aplicación Pilar Basic 4.3, resultado de la adaptación a la metodología ENISA de la herramienta EAR Pilar, ideada como herramienta de ayuda en la realización de los cálculos asociados al análisis de riesgos en sistemas complejos.

4. PERFIL DE RIESGO

La definición del perfil de riesgo según la metodología ENISA se realiza en base a la definición de la situación de la organización de acuerdo a las siguientes áreas y niveles:

Áreas de riesgo	Alto	Medio	Bajo
Riesgos jurídicos	La empresa maneja información de los clientes de carácter sensible y personal, incluidas historias médicas y datos personales críticos, con arreglo a lo previsto en la legislación de protección de datos de la UE	La empresa maneja la información de los clientes de índole personal, pero no sensible, conforme se define ésta en la Ley de protección de datos de la UE	La empresa no maneja datos personales distintos a los del personal empleado por ella
Riesgos de productividad	La empresa emplea a más de 100 personas que requieren a diario del acceso a aplicaciones y servicios empresariales	La empresa emplea a más de 50 personas que requieren a diario del acceso a aplicaciones y servicios empresariales	La empresa emplea a menos de 10 personas que requieren a diario del acceso a aplicaciones y servicios empresariales
Riesgos para la estabilidad financiera	Los ingresos anuales exceden de 25 millones de euros y/o las transacciones financieras con terceros o clientes tienen lugar como proceso habitual parte de su actividad empresarial	Los ingresos anuales no exceden de 25 millones de euros	Los ingresos anuales no exceden de 5 millones de euros
Riesgos para la reputación y de pérdida de confianza de los clientes	La indisponibilidad o la calidad del servicio repercuten directamente en el perfil empresarial, y/o más del 70% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa	La indisponibilidad o la calidad del servicio pueden repercutir indirectamente en el perfil empresarial, y/o menos del 5% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa	La indisponibilidad o la calidad del servicio no pueden repercutir de manera directa o indirecta en el perfil empresarial, ni derivar en pérdida de ingresos

Tabla 1: Criterios de definición del perfil de riesgos

En el caso que nos ocupa, la empresa A centra su actividad en XXXX[3]

[3] Here there come the comments over the reasons why we chose the risk profile based on the table about and the answers made to questions in the questionnaire and another one regarded with the SME business environment

Por lo tanto de acuerdo a las características de la empresa analizada y en base a los criterios definidos en la metodología ENISA de análisis de riesgos y según la percepción de la propia empresa, se pueden determinar los niveles de riesgo que se muestran en la siguiente tabla, siendo el valor más alto y el que determina el perfil de riesgo global de la empresa "**Medio**"[4]

Áreas de riesgo	Nivel de riesgo	Perfil de Riesgo
Riesgos jurídicos (*Legal and Regulatory*)	Medio (*Medium*)	Medio *(Medium)*
Riesgos de productividad (*Productivity*)	Bajo *(Low)*	
Riesgos para la estabilidad financiera (*Financial Stability*)	Bajo *(Low)*	
Riesgos para la reputación y de pérdida de confianza de los clientes (*Reputation and Loss of Customer Confidence*)	Medio *(Medium)*	

Tabla 2: Perfil de riesgo de la empresa

[4] Risk profile selection for each defined risk area

5. ACTIVOS CRÍTICOS

Tal y como se ha explicado en el apartado anterior, se han identificado dos actividades críticas para la empresa A[5]:

- XXXXXXXX
- XXXXXXXX

De forma adicional se puede destacar que la empresa dispone de portal web y servicio de correo electrónico en régimen de hosting.

Teniendo en cuenta los datos anteriores y la entrevista mantenida con los responsables de la empresa se han identificado y clasificado los siguientes activos críticos que serán incluidos en el análisis de riesgos:[6]

- Aplicaciones (*Applications*):
  - [Source code version control]
  - [Financial Control]
  - [CRM]
- Equipos (*Systems*)
  - [Web Server]
  - [Archiving and Backup Server]
  - [Firewall, pabx and monitoring Server]
  - [Web and mail hosting Server]
  - [workstations]
- Comunicaciones (*Network*)
  - [Cabling, routers and network segments]
- Personal (*People*)
  - [Research and development]
  - [Operation and technology]
  - [Sales and marketing]
  - [Administrative assistants and human resources management]
  - [Super administrator role: IT administration, operation and technology, research and development]

[5] Critical Business activities identification

[6] Assets identification

De acuerdo a la metodología ENISA los activos enumerados pueden englobarse dentro de las siguientes categorías:[7]

Activo crítico (Critical Asset)	Categoría de activo (*Asset category*)	Componentes (*Components*)	Requisitos de seguridad (*Security requirements*)	Justificación de su selección (*Justification*)
Desarrollo y Diseño de sistemas Monitorización de instalaciones de clientes (*Research and development,* *Customers infrastructure monitoring*)	Sistemas (*Systems*)	Todos los activos definidos en este apartado	Confidencialidad (Confidentiality) Disponibilidad (Availability)	XXXXX

Tabla 3: Activos seleccionados

[7] Assets categorization and security requirements identification

6. SELECCIÓN DE CONTROLES

La metodología ENISA define una serie de salvaguardas organizativas y orientadas a activos que deben seleccionarse o que son recomendables según el perfil de riesgo de la empresa y los activos críticos de la misma.

Según el perfil de riesgo definido para cada una de las áreas y teniendo en cuenta las especificaciones de la metodología ENISA se pueden seleccionar los siguientes controles:[8]

Áreas de riesgo (*Risk areas*)	Nivel de riesgo (*Risk level*)	Controles organizativos (*Organizational controls*)
Riesgos jurídicos (*Legal and Regulatory*)	Medio (*Medium*)	SP1 SP4
Riesgos de productividad (*Productivity*)	Bajo (*Low*)	SP4.1
Riesgos para la estabilidad financiera (*Financial Stability*)	Bajo (*Low*)	SP4.1
Riesgos para la reputación y de pérdida de confianza de los clientes (*Reputation and Loss of Customer Confidence*)	Medio (*Medium*)	SP4 SP1

Tabla 4: Salvaguardas organizativas recomendadas

[8] Organizational controls

Basándonos en el perfil de riesgos global y la categorización de los activos, según la metodología ENISA se deben seleccionar los controles pertenecientes al grupo CC-2S que agrupa las siguientes salvaguardas:[9]

Identificación de la tarjeta de controles basados en los activos (*Asset Bases Control card ID*)										CC-2S
Perfil de riesgos (*Risk profile*)										Medio
Categoría del activo (*Asset category*)										Sistema
Requisitos de seguridad (*Security requirements*)	Seguridad Física (*Physical Security*)	Gestión de sistemas y redes (*System and network Management*)	Herramientas de administración de sistemas (*System Administration tools*)	Seguimiento y auditoría de la seguridad física (*Monitoring and Auditing IT Security*)	Autenticación y autorización (*Authenticatioon and Authorization*)	Gestión de vulnerabilidades (*Vulnerability Management*)	Cifrado (*Encryption*)	Diseño y arquitectura de seguridad (*Securioty Architecture and Design*)	Gestión de incidentes (*Incident Management*)	Prácticas de personal generales (*General Staff practices*)
Confidencialidad (*Condifentiality*)		OP2.1.6 OP2.1.7			OP2.4.1					
Integridad (*Integrity*)		OP2.1.9			OP2.4.1					
Disponibilidad (*Availability*)		OP2.1.6 OP2.1.7								

Tabla 5: Salvaguardas orientada a activos recomendadas

[9] Score card selection and asset based controls

De esta forma se pueden concluir los siguientes controles a implantar en el sistema:

Activo	Control	Justificación de su selección
Controles basados en los activos	OP2.1.6 OP2.1.7 OP2.4.1	Los controles de autenticación y autorización, así como los de gestión de red son esenciales para mantener la disponibilidad y confidencialidad del activo objeto en consideración
Controles organizativos	SP1	Formación y sensibilización en materia de seguridad
	SP4	Política de seguridad
	SP4.1	Incluido en el SP4

Tabla 6: Salvaguardas recomendadas

En los siguientes aparatados del presente documento se profundiza en los aspectos incluidos en cada una de los controles recomendados, así como en el análisis entre el estado actual de implantación y el nivel recomendado de los mismos.

7. ANÁLISIS DEL ESTADO ACTUAL VS OBJETIVO

Con el objetivo de realizar una gestión y priorización adecuada de los controles seleccionados, se debe realizar un análisis que nos permita contrastar el estado actual de aplicación de las diferentes salvaguardas en la organización respecto el estado recomendable de las mismas. Para facilitar la realización de este análisis se ha dividido el grado de implantación de las salvaguardas según los siguientes niveles[10]:

- L0. La salvaguarda no se encuentra implantada en la organización.
- L1. En este nivel de madurez, las salvaguardas existen, pero no se gestionan. El éxito depende de buena suerte. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta.
- L2. En este nivel de madurez, la eficacia de las salvaguardas depende de la buena suerte y de la buena voluntad de las personas. Los éxitos son repetibles, pero no hay plan para los incidentes más allá de la reacción heroica. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.
- L3. Se despliegan y se gestionan las salvaguardas. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular de las protecciones. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece.
- L4. Usando medidas de campo, la dirección puede controlar empíricamente la eficacia y la efectividad de las salvaguardas. En particular, la dirección puede fijar metas cuantitativas de la calidad. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa, mientras que en el nivel L3, la confianza era solamente cualitativa.
- L5. Este nivel de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora de los procesos. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.

De esta forma, en las siguientes tablas se plasma para cada una de los grupos de salvaguarda la comparativa entre el estado actual y el estado objetivo o recomendable según el modelado de la metodología ENISA realizado mediante la herramienta Pilar. Las valoraciones asignadas a cada una de las salvaguardas tanto para el estado actual como el objetivo son fruto de la entrevista mantenida con la empresa y la experiencia de la empresa GMV en la realización de análisis de riesgos.

[10] Here comes by safeguard, the tables with the current situation and the regarded situation as ENISA suggests. we have done a gap analysis considering the current situation based on the meeting held with the SME. the maturity level for each control has been evaluated in six levels l0-l5 in order to simplify the gap analysis.

For each table with the safeguards and the evaluation, we have made comments with the justification or any finding that echoes the evidence if required.

[SP1] Formación y sensibilización en materia de seguridad

salvaguarda	[presente]	[objetivo]
[SP1.1] Los miembros del personal comprenden sus funciones y responsabilidades en materia de seguridad. Este hecho está documentado y comprobado.	L3	L3
[SP1.2] Se dispone de conocimientos técnicos internos adecuados para la totalidad de servicios, mecanismos y tecnologías empleados (p. ej., registro, seguimiento o codificación), incluido el funcionamiento de éstos en condiciones de seguridad. Este hecho está documentado y comprobado.	L4	L3
[SP1.3] Se imparten a todo el personal conocimientos y formación y se le envían recordatorios periódicos en materia de seguridad. El conocimiento del personal está documentado, y la conformidad se comprueba periódicamente. La formación comprende los temas que siguen:	L1	L3
estrategias, metas y objetivos en materia de seguridad	L2	L3
reglamentos, políticas y procedimientos de seguridad	L3	L3
políticas y procedimientos de colaboración con terceros	L1	L3
planes para contingencias y recuperación en caso de catástrofe	L1	L3
requisitos relativos a la seguridad física	L3	L3
perspectiva de los usuarios respecto a	L2	L3
la gestión de sistemas y redes	L2	L3
las herramientas de administración del sistema	L2	L3
el seguimiento y la auditoría en lo que atañe a la seguridad física y asociada a las tecnologías de la información	L2	L3
autenticación y autorización	L2	L3
gestión de vulnerabilidades	L2	L3
codificación	L2	L3
arquitectura y diseño	L2	L3
gestión de incidentes	L1	L3
prácticas generales de personal	L2	L3
observancia de la legislación, sanciones y actuaciones disciplinarias por infracciones de la seguridad	L2	L3
modo de acceder correctamente a la información sensible y trabajo en las áreas en las que ésta es accesible	L3	L3
políticas y procedimientos de extinción de la relación laboral en lo que atañe a la seguridad	L1	L3

Comentarios:[11]

[11] Regarded comments. Example: Staff members apply common security practices based on their own knowledge. These practices are not documented or linked with internal policy or employee's contracts.

Organization common security practices should be documented and included in the internal training program. In addition, staff members should sign non disclosure agreements at the beginning of working relationship. …

[SP4] Políticas y normativas de seguridad

salvaguarda	[presente]	[objetivo]
[SP4.1] La organización dispone de un conjunto exhaustivo de políticas vigentes y documentadas que se revisan y actualizan periódicamente. Estas políticas abordan áreas temáticas fundamentales en materia de seguridad, entre las que se cuentan:	L1	L2
la gestión y la estrategia de seguridad	L1	L2
la gestión de riesgos para la seguridad	L1	L2
la seguridad física	L1	L2
la gestión de sistemas y redes	L2	L2
las herramientas de administración de sistemas	L3	L2
el seguimiento y la auditoría	L2	L2
la autenticación y la autorización	L1	L2
la gestión de vulnerabilidades	L1	L2
la codificación	L1	L2
la arquitectura y el diseño de la seguridad	L1	L2
la gestión de incidentes	L1	L2
las prácticas de seguridad de personal	L2	L2
la legislación aplicable	L3	L2
la sensibilización y la formación	L2	L2
la seguridad de la información basada en la colaboración	L1	L2
la planificación de contingencias y la recuperación en caso de catástrofe	L1	L2
[SP4.2] Existe un proceso documentado para la gestión de políticas de seguridad, incluidas las tareas de:	L1	L2
creación	L1	L2
administración (incluidas revisiones y actualizaciones periódicas)	L1	L2
comunicación	L1	L2
[SP4.3] La organización cuenta con un proceso documentado para la evaluación periódica (técnica y no técnica) del cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L1	L3
[SP4.4] La organización cuenta con un proceso documentado para garantizar el cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L1	L3
[SP4.5] La organización aplica de manera uniforme sus políticas de seguridad.	L2	L3
[SP4.6] Únicamente el personal autorizado puede comprobar y revisar las políticas y procedimientos de seguridad.	L3	L3

Comentarios:

[OP2] Seguridad de las tecnologías de la información

salvaguarda	[presente]	[objetivo]
[OP2.1.6] Existe un plan de copias de respaldo de datos que	L2	L3
se actualiza regularmente	L2	L3
se comprueba periódicamente	L2	L3
requiere la realización de copias de respaldo programadas regularmente, tanto del software, como de los datos	L2	L3
requiere la comprobación y verificación periódicas de la capacidad para restaurar a partir de copias de respaldo	L2	L3
[OP2.1.7] Todo el personal comprende y es capaz de desempeñar sus responsabilidades con arreglo a los planes de respaldo.	L2	L3

[OP2.4.1] Se utilizan controles de acceso y mecanismos de autenticación de usuario apropiados (p. ej., permisos de archivo, configuración de red) coherentes con la política establecida al respecto, con el fin de restringir el acceso de los usuarios a	L2	L3
la información	L2	L3
las utilidades del sistema	L2	L3
el código fuente de programas	L2	L3
los sistemas sensibles	L2	L3
determinadas aplicaciones y servicios	L2	L3
conexiones de red en la organización	L2	L3
conexiones de red con origen fuera de la organización	L2	L3

Comentarios:

8. RESUMEN EJECUTIVO

XXXXX[12]

[12] Here comes the most important aspects and recommendations that the SME should take into account with regard to ENISA risk analysis approach and GMV expertise. it includes recommendations about the selected scorecards in ENISA methodology and other relevant aspects

9. ANEXO A: RESULTADOS DE LA HERRAMIENTA PILAR

La herramienta Pilar permite completar los resultados de la metodología ENISA con consideraciones más específicas de análisis de riesgos, enriqueciendo los resultados obtenidos con datos más específicos y gráficos que permiten contrastar de forma rápida y sencilla la evolución del riesgo en la organización respecto al grado de implantación de las salvaguardas.

En cuanto a la selección de amenazas, la herramienta Pilar permite definir las amenazas de interés para cada uno de los activos. Cada una de estas amenazas tendrá asociados unos parámetros de impacto para cada una de las dimensiones de seguridad en caso de materialización y frecuencia de ocurrencia. En la versión utilizada de la herramienta para el desarrollo del piloto, se seleccionan unas amenazas por defecto para cada tipo de activo según su naturaleza, personas, red, hardware, ..., con valores también por defecto para la frecuencia y el impacto. Esto permite al usuario abstraerse de la complejidad asociada a la selección de este tipo de parámetros durante el análisis de riesgos a la vez que se permite desglosar la información del mapa de riesgo por cada una de las amenazas asociadas a los activos. De forma complementaria a las amenazas seleccionadas por defecto la herramienta permite seleccionar amenazas adicionales que permitan adaptarse a los diferentes requisitos del sector de actividad de cada empresa. Las amenazas por defecto para cada uno de los activos que han sido seleccionadas en la herramienta son las siguientes:

Aplicaciones
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.19] Escapes de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.14] Interceptación de información (escucha)
[A.22] Manipulación de programas

Tabla 7: Amenazas de aplicaciones

Equipos
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico

[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.19] Escapes de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.14] Interceptación de información (escucha)
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo

Tabla 8: Amenazas de equipos

Comunicaciones
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia

[E.19] Escapes de información
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.14] Interceptación de información (escucha)
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo

Tabla 9: Amenazas de comunicaciones

Personas
[E.7] Deficiencias en la organización
[E.19] Escapes de información
[E.28] Indisponibilidad del personal
[A.19] Divulgación de información
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)

Tabla 10: Amenazas de personas

En cuanto al mapa de riesgos, la herramienta permite representar de forma gráfica el riesgo presente en la organización en diferentes momentos en función del estado de implantación de las salvaguardas en dichos momentos. En el desarrollo del piloto se han analizado las siguientes estados:[13]

- Riesgo potencial: Riesgo en caso de no existir implantada ninguna salvaguarda.
- Riesgo presente: Riesgo existente en la organización con el estado de implantación actual de las salvaguardas.
- Riesgo objetivo: Riesgo existente en la organización si se implantasen las salvaguardas recomendadas por la metodología ENISA y aquellas recomendaciones fruto de la experiencia de la empresa GMV y los aspectos analizados durante las entrevistas mantenidas con la empresa.

Cada uno de estos mapas de riesgo pueden observarse en las siguientes figuras.

[13] Here comes the potential risk, current risk and target risk images obtained from pilar tool for each SME.

	[D]	[I]	[C]
ACTIVOS	(6.3)	(6.3)	(6.3)
[SW] Aplicaciones	(5.9)	(6.3)	(6.3)
[ ]	(5.9)	(6.3)	(6.3)
[ ]	(5.9)	(6.3)	(6.3)
[ ]	(5.9)	(6.3)	(6.3)
[HW] Equipos	(6.3)	(6.3)	(6.3)
[ ]	(6.3)	(6.3)	(6.3)
[ ]	(6.3)	(5.6)	(5.6)
[ ]	(5.6)	(3.3)	(5.3)
[ ]	(6.3)	(6.3)	(6.3)
[ ]	(6.3)	(3.6)	(5.0)
[COM] Comunicaciones	(5.9)	(3.3)	(5.3)
[ ]	(5.9)	(3.3)	(5.3)
[P] Personal	(4.3)	(4.9)	(5.0)
[ ]	(4.3)	(4.9)	(5.0)
[ ]	(4.3)	(4.9)	(5.0)
[ ]	(4.0)	(3.5)	(3.6)
[ ]	(4.0)	(3.5)	(3.6)
[ ]	(4.3)	(4.9)	(5.0)

Figura 3: Riesgo potencial

	[D]	[I]	[C]
ACTIVOS	(3.9)	(3.9)	(3.8)
[SW] Aplicaciones	(3.6) [D] Disponibilidad	(3.9)	(3.8)
[ ]	(3.6)	(3.9)	(3.8)
[ ]	(3.6)	(3.9)	(3.8)
[ ]	(3.6)	(3.9)	(3.8)
[HW] Equipos	(3.9)	(3.8)	(3.8)
[ ]	(3.9)	(3.8)	(3.8)
[ ]	(3.9)	(3.2)	(3.3)
[ ]	(3.3)	(0.9)	(3.1)
[ ]	(3.9)	(3.8)	(3.8)
[ ]	(3.9)	(1.2)	(2.7)
[COM] Comunicaciones	(3.6)	(0.9)	(3.0)
[ ]	(3.6)	(0.9)	(3.0)
[P] Personal	(1.9)	(2.5)	(2.7)
[ ]	(1.9)	(2.5)	(2.7)
[ ]	(1.9)	(2.5)	(2.7)
[ ]	(1.7)	(1.1)	(1.2)
[ ]	(1.7)	(1.1)	(1.2)
[ ]	(1.9)	(2.5)	(2.7)

Figura 4: Riesgo Presente

	[D]	[I]	[C]
ACTIVOS	{1.7}	{1.6}	{1.6}
[SW] Aplicaciones	{1.4}	{1.6}	{1.6}
[ ]	{1.4}	{1.6}	{1.6}
[ ]	{1.4}	{1.6}	{1.6}
[ ]	{1.4}	{1.6}	{1.6}
[HW] Equipos	{1.7}	{1.5}	{1.5}
[ ]	{1.7}	{1.5}	{1.5}
[ ]	{1.7}	{0.9}	{0.9}
[ ]	{1.0}	{0.0}	{0.6}
[ ]	{1.7}	{1.5}	{1.5}
[ ]	{1.7}	{0.0}	{0.7}
[COM] Comunicaciones	{1.3}	{0.0}	{0.5}
[ ]	{1.3}	{0.0}	{0.5}
[P] Personal	{0.0}	{0.5}	{0.6}
[ ]	{0.0}	{0.5}	{0.6}
[ ]	{0.0}	{0.5}	{0.6}
[ ]	{0.0}	{0.0}	{0.0}
[ ]	{0.0}	{0.0}	{0.0}
[ ]	{0.0}	{0.5}	{0.6}

Figura 5: Riesgo objetivo

En el proyecto de la herramienta Pilar proporcionado a la empresa se pueden desglosar cada uno de los mapas de riesgo anteriores en función de las distintas amenazas.

Adicionalmente, el análisis completo de implantación de salvaguardas que se ha tenido en cuenta para la obtención de los mapas de riesgo anteriores se presenta en el Anexo B del presente documento.

10. ANEXO B: ESTADO DE IMPLANTACIÓN DE SALVAGUARDAS[14]

[SP1] Formación y sensibilización en materia de seguridad

salvaguarda	[presente]	[objetivo]
[SP1.1] Los miembros del personal comprenden sus funciones y responsabilidades en materia de seguridad. Este hecho está documentado y comprobado.	L3	L3
[SP1.2] Se dispone de conocimientos técnicos internos adecuados para la totalidad de servicios, mecanismos y tecnologías empleados (p. ej., registro, seguimiento o codificación), incluido el funcionamiento de éstos en condiciones de seguridad. Este hecho está documentado y comprobado.	L4	L3
[SP1.3] Se imparten a todo el personal conocimientos y formación y se le envían recordatorios periódicos en materia de seguridad. El conocimiento del personal está documentado, y la conformidad se comprueba periódicamente. La formación comprende los temas que siguen:	L1	L3
estrategias, metas y objetivos en materia de seguridad	L2	L3
reglamentos, políticas y procedimientos de seguridad	L3	L3
políticas y procedimientos de colaboración con terceros	L1	L3
planes para contingencias y recuperación en caso de catástrofe	L1	L3
requisitos relativos a la seguridad física	L3	L3
perspectiva de los usuarios respecto a	L2	L3
la gestión de sistemas y redes	L2	L3
las herramientas de administración del sistema	L2	L3
el seguimiento y la auditoría en lo que atañe a la seguridad física y asociada a las tecnologías de la información	L2	L3
autenticación y autorización	L2	L3
gestión de vulnerabilidades	L2	L3
codificación	L2	L3
arquitectura y diseño	L2	L3
gestión de incidentes	L1	L3
prácticas generales de personal	L2	L3
observancia de la legislación, sanciones y actuaciones disciplinarias por infracciones de la seguridad	L2	L3
modo de acceder correctamente a la información sensible y trabajo en las áreas en las que ésta es accesible	L3	L3
políticas y procedimientos de extinción de la relación laboral en lo que atañe a la seguridad	L1	L3

Comentarios:

[14] Here comes by safeguard, the tables with the current situation and the target situation. in this section, we have included the gap analysis for safeguards not suggested by ENISA approach but GMV consider that are important controls to take into account by the SME.

[SP2] Estrategia de seguridad

salvaguarda	[presente]	[objetivo]
[SP2.1] Las estrategias empresariales de la organización incorporan de manera rutinaria consideraciones de seguridad.	L3	L3
[SP2.2] En las estrategias y políticas de seguridad se tienen en cuenta las estrategias y objetivos empresariales de la organización.	L3	L3
[SP2.3] Las estrategias, metas y objetivos en materia de seguridad se documentan y se revisan, actualizan y comunican periódicamente a la organización.	L2	L2

[SP3] Gestión de seguridad

salvaguarda	[presente]	[objetivo]
[SP3.1] La dirección asigna fondos y recursos suficientes a las actividades de seguridad de la información.	L2	L2
[SP3.2] Se definen funciones y responsabilidades en materia de seguridad para todo el personal de la organización.	L2	L2
[SP3.3] En las prácticas de la organización en materia de contratación y de extinción de la relación laboral con el personal se tienen en cuenta las cuestiones de seguridad de la información.	L1	L1
[SP3.4] Los niveles requeridos de seguridad de la información y el modo en que se aplican a personas y grupos se documentan y aplican.	L1	L1
[SP3.5] La organización gestiona los riesgos que atañen a la seguridad de la información, con inclusión de:	L1	L1
la evaluación de los riesgos para la seguridad de la información, tanto periódicamente, como en respuesta a cambios significativos en la tecnología, amenazas internas o externas, o los sistemas y operaciones de la organización	L2	L2
la adopción de medidas para mitigar los riesgos hasta alcanzar un nivel aceptable	L1	L1
el mantenimiento de un nivel de riesgos aceptable	L1	L1
la utilización de evaluaciones de riesgos para la seguridad de la información con el fin de facilitar la selección de medidas de seguridad y control rentables, equilibrando los costes de ejecución con las posibles pérdidas	L1	L1
[SP3.6] La dirección recibe informes rutinarios, y actúa basándose en ellos, en los que se resumen los resultados de:	L2	L2
la revisión de los registros de sistema	L2	L2
la revisión de los historiales de auditoría	L2	L2
las evaluaciones de vulnerabilidades tecnológicas	L2	L2
los incidentes de seguridad y las respuestas dadas a los mismos	L2	L2
las evaluaciones de riesgos	L2	L2
las revisiones de la seguridad física	L2	L2
los planes y recomendaciones para la mejora de la seguridad	L2	L2

[SP4] Políticas y normativas de seguridad

salvaguarda	[presente]	[objetivo]
[SP4.1] La organización dispone de un conjunto exhaustivo de políticas vigentes y documentadas que se revisan y actualizan periódicamente. Estas políticas abordan áreas temáticas fundamentales en materia de seguridad, entre las que se cuentan:	L1	L2
la gestión y la estrategia de seguridad	L1	L2
la gestión de riesgos para la seguridad	L1	L2
la seguridad física	L1	L2
la gestión de sistemas y redes	L2	L2
las herramientas de administración de sistemas	L3	L2
el seguimiento y la auditoría	L2	L2
la autenticación y la autorización	L1	L2
la gestión de vulnerabilidades	L1	L2
la codificación	L1	L2
la arquitectura y el diseño de la seguridad	L1	L2
la gestión de incidentes	L1	L2
las prácticas de seguridad de personal	L2	L2
la legislación aplicable	L3	L2
la sensibilización y la formación	L2	L2
la seguridad de la información basada en la colaboración	L1	L2
la planificación de contingencias y la recuperación en caso de catástrofe	L1	L2
[SP4.2] Existe un proceso documentado para la gestión de políticas de seguridad, incluidas las tareas de:	L1	L2
creación	L1	L2
administración (incluidas revisiones y actualizaciones periódicas)	L1	L2
comunicación	L1	L2
[SP4.3] La organización cuenta con un proceso documentado para la evaluación periódica (técnica y no técnica) del cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L1	L3
[SP4.4] La organización cuenta con un proceso documentado para garantizar el cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L1	L3
[SP4.5] La organización aplica de manera uniforme sus políticas de seguridad.	L2	L3
[SP4.6] Únicamente el personal autorizado puede comprobar y revisar las políticas y procedimientos de seguridad.	L3	L3

Comentarios:

[SP5] Gestión de la seguridad en régimen de colaboración

salvaguarda	[presente]	[objetivo]
[SP5.1] La organización ha procedido a la documentación, el seguimiento y la ejecución de procedimientos para la protección de su información cuando colabora con entidades externas (p. ej., terceros, colaboradores, subcontratistas o socios).	L2	L2
[SP5.2] La organización ha comprobado que los servicios, mecanismos y tecnologías de seguridad externalizados satisfacen sus necesidades y requisitos.	L2	L2
[SP5.3] La organización documenta, supervisa y aplica estrategias de protección de la información perteneciente a entidades externas a la que se accede desde componentes de su infraestructura, o que es utilizada por su personal.	L2	L2
[SP5.4] La organización ofrece y verifica actividades de sensibilización y formación sobre las políticas y los procedimientos de seguridad de entidades externas para el personal que interactúa con éstas.	n.a.	n.a.
[SP5.5] Existen procedimientos documentados respecto al personal externo cuya relación con la organización ha concluido, en los que se especifican las medidas de seguridad pertinentes para finalizar su posibilidad de acceso. Estos procedimientos se comunican a la organización externa y se coordinan con ella.	n.a.	n.a.

[SP6] Planificación de contingencias / recuperación en caso de catástrofe

salvaguarda	[presente]	[objetivo]
[SP6.1] Se ha efectuado un análisis de operaciones, aplicaciones y de la significación de los datos.	L1	L1
[SP6.2] La organización ha documentado	L1	L1
los planes de continuidad de la actividad empresarial y de operación en casos de emergencia	L1	L1
los planes de recuperación en caso de catástrofe	L1	L1
los planes de contingencia para la respuesta en casos de emergencia	L1	L1
[SP6.3] En los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial se consideran los requisitos y conrtroles de acceso físico y electrónico.	L1	L1
[SP6.4] Los planes de contingencia, recuperación en caso de catástrofe, y continuidad de la actividad empresarial se revisan y comprueban periódicamente.	L1	L1
[SP6.5] Todo el personal ...	L1	L1
tiene conocimiento de los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial	L1	L1
comprende sus responsabilidades y está capacitado para cumplirlas	L1	L1

[OP1] Seguridad física

salvaguarda	[presente]	[objetivo]
[OP1.1] Planes y procedimientos de seguridad física	L0	L2

[OP1.1.1] Existen planes de seguridad de las instalaciones documentados, concebidos para salvaguardar locales, edificios y cualquier otra área restringida.	L2	L2
[OP1.1.2] Estos planes se revisan, comprueban y actualizan periódicamente.	L1	L2
[OP1.1.3] Los procedimientos y mecanismos de seguridad física se comprueban y revisan periódicamente.	L1	L2
[OP1.1.4] Existen políticas y procedimientos documentados para la gestión de visitantes, que incluyen	L2	L2
el registro en la entrada	L2	L2
el acompañamiento por las instalaciones	L2	L2
los registros de acceso	L2	L2
la recepción y los servicios de hospitalidad	L2	L2
[OP1.1.5] Existen políticas y procedimientos documentados para el control físico del hardware y el software, incluidos	L0	L2
terminales, portátiles, módem, componentes inalámbricos y todos los demás elementos utilizados para acceder a la información	L1	L2
el acceso, el almacenamiento y la recuperación de copias de seguridad de datos	L2	L2
el almacenamiento de información sensible en medios físicos y electrónicos	L1	L2
la supresión de información sensible, o de los medios en los que se encuentra almacenada	L0	L2
la reutilización y el reciclaje de papel y medios electrónicos.	L0	L2
[OP1.2] Control de acceso físico	L1	L3
[OP1.2.1] Existen políticas y procedimientos documentados respecto al acceso individual y en grupo, que comprenden:	L1	L3
las normas de concesión del nivel pertinente de acceso físico	L1	L3
las normas para la determinación de los derechos iniciales de acceso	L1	L3
la modificación del derecho de acceso	L1	L3
la anulación del derecho de acceso	L1	L3
la revisión y la comprobación periódicas de los derechos de acceso	L1	L3
[OP1.2.2] Existen políticas, procedimientos y mecanismos documentados para controlar el acceso físico a entidades definidas. Se incluyen aquí:	L1	L3
áreas de trabajo	L1	L3
medios de hardware (ordenadores, dispositivos de comunicación, etc.) y de software	L1	L3
[OP1.2.3] Existen procedimientos documentados para verificar la autorización de acceso antes de autorizar el acceso físico.	L2	L3
[OP1.2.4] Los terminales y otros componentes que permiten el acceso a información sensible se encuentran físicamente protegidos con el fin de evitar accesos no autorizados.	L1	L3
[OP1.3] Seguimiento y auditoría de la seguridad física	L1	L3
[OP1.3.1] Se conservan registros de mantenimiento para documentar las reparaciones y modificaciones de los componentes físicos de las instalaciones.	L1	L3
[OP1.3.2] Pueden justificarse las acciones de una persona o de un grupo respecto a la totalidad de medios controlados físicamente.	L1	L3
[OP1.3.3] Se examinan regularmente registros de auditoría y seguimiento para detectar anomalías, y se emprenden acciones correctivas en caso necesario.	L1	L3

Comentarios:

[OP2] Seguridad de las tecnologías de la información

salvaguarda	[presente]	[objetivo]
[OP2.1] Gestión de sistemas y redes	L1	L2
[OP2.1.1] Existen planes de seguridad documentados para la salvaguarda de sistemas y redes.	L3	L3
[OP2.1.2] Los planes de seguridad se revisan, comprueban y actualizan periódicamente.	L2	L2
[OP2.1.3] Se protege la información sensible mediante su almacenamiento en condiciones de seguridad, como el que proporcionan	L1	L2
las cadenas de custodia definidas	L2	L2
las copias de respaldo almacenadas fuera de las instalaciones	L3	L2
los medios de almacenamiento separables	L2	L2
un proceso de eliminación de la información sensible o de sus medios de almacenamiento	L1	L2
[OP2.1.4] La integridad del software instalado se verifica regularmente.	L1	L3
[OP2.1.5] Todos los sistemas se encuentran actualizados respecto a revisiones, parches, y recomendaciones en documentos de asesoramiento sobre seguridad.	L1	L3
[OP2.1.6] Existe un plan de copias de respaldo de datos que	L2	L2
se actualiza regularmente	L2	L2
se comprueba periódicamente	L2	L2
requiere la realización de copias de respaldo programadas regularmente, tanto del software, como de los datos	L2	L2
requiere la comprobación y verificación periódicas de la capacidad para restaurar a partir de copias de respaldo	L2	L2
[OP2.1.7] Todo el personal comprende y es capaz de desempeñar sus responsabilidades con arreglo a los planes de respaldo.	L2	L3
[OP2.1.8] Los cambios del hardware y el software de las TI se planifican, supervisan y documentan.	L2	L3
[OP2.1.9] Los miembros del personal de TI siguen los procedimientos pertinentes al publicar, modificar y anular contraseñas, cuentas y privilegios de usuario.	L2	L2
Se requiere una identificación única de usuario para todos los usuarios del sistema de información, incluidos los usuarios terceros.	L2	L2
Las cuentas y contraseñas por defecto han sido suprimidas de los sistemas.	L2	L2
[OP2.1.10] Sólo operan en los sistemas los servicios necesarios; todos los innecesarios se han suprimido.	L3	L3
[OP2.2] Herramientas de administración de sistemas	L1	L2
[OP2.2.1] Los nuevos instrumentos de seguridad, procedimientos y mecanismos se revisan de manera ordinaria para determinar su aplicabilidad en la consecución de las estrategias de seguridad de la organización.	L1	L2
[OP2.2.2] Las herramientas y los mecanismos para conseguir el uso de una administración de sistemas y de red segura, y su revisión y actualización o sustitución con carácter periódico. Son ejemplos de estas herramientas los que siguen:	L2	L2
comprobadores de la integridad de los datos	L2	L2
herramientas de codificación	L2	L2

escáneres de vulnerabilidades	L2	L2
herramientas de comprobación de la calidad de las contraseñas	L2	L2
escáneres de virus	L2	L2
herramientas de gestión de procesos	L2	L2
sistemas de detección de intrusos	L2	L2
administraciones remotas seguras	L2	L2
herramientas de servicio de red	L2	L2
analizadores de tráfico	L2	L2
herramientas de respuesta en caso de incidente	L2	L2
herramientas forenses para el análisis de datos	L2	L2
[OP2.3] Seguimiento y auditoría de la seguridad física	L1	L2
[OP2.3.1] La organización utiliza de manera ordinaria herramientas de seguimiento y auditoría de sistemas y redes.	L1	L2
La actividad es objeto de seguimiento por parte del personal de TI.	L1	L2
Se registra la actividad de sistemas y redes.	L1	L2
Los registros se revisan regularmente.	L1	L2
La actividad inusual se trata con arreglo a la política o el procedimiento pertinentes.	L1	L2
Las herramientas se revisan y actualizan periódicamente.	L1	L2
[OP2.3.2] Los cortafuegos y otros componentes de seguridad se auditan periódicamente para determinar su conformidad con la política pertinente.	L1	L2
[OP2.4] Autenticación y autorización	L0	L3
[OP2.4.1] Se utilizan controles de acceso y mecanismos de autenticación de usuario apropiados (p. ej., permisos de archivo, configuración de red) coherentes con la política establecida al respecto, con el fin de restringir el acceso de los usuarios a	L2	L3
la información	L2	L3
las utilidades del sistema	L2	L3
el código fuente de programas	L2	L3
los sistemas sensibles	L2	L3
determinadas aplicaciones y servicios	L2	L3
conexiones de red en la organización	L2	L3
conexiones de red con origen fuera de la organización	L2	L3
[OP2.4.2] Existen políticas y procedimientos de uso de la información documentados respecto al acceso individual y en grupo con el fin de:	L2	L3
establecer las normas de concesión del nivel pertinente de acceso	L2	L3
establecer un derecho inicial de acceso	L2	L3
modificar el derecho de acceso	L2	L3
anular el derecho de acceso	L2	L3
revisar y comprobar periódicamente los derechos de acceso	L2	L3
[OP2.4.3] Los métodos y mecanismos de control de acceso restringen el acceso a los recursos con arreglo a los derechos determinados en políticas y procedimientos.	L2	L4
[OP2.4.4] Los métodos y mecanismos de control de acceso se revisan y comprueban periódicamente.	L1	L3
[OP2.4.5] Se dotan métodos o mecanismos para garantizar que la información sensible no es objeto de acceso, alteración o destrucción de un modo no autorizado.	L2	L3
[OP2.4.6] Se utilizan mecanismos de autenticación para proteger la disponibilidad, integridad y confidencialidad de la información sensible. Son ejemplos de estos instrumentos los que siguen:	L0	L3

las firmas digitales	L0	L3
la biometría	L0	L3
[OP2.5] Gestión de vulnerabilidades	L1	L2
[OP2.5.1] Existe un conjunto documentado de procedimientos para la gestión de vulnerabilidades, entre los que figuran:	L2	L2
la selección de herramientas de evaluación de vulnerabilidades, listas de comprobación y scripts	L2	L2
el mantenimiento al día respecto a los tipos de vulnerabilidades conocidos y los métodos de ataque	L2	L2
la revisión de fuentes de información sobre anuncios de vulnerabilidad, alertas de seguridad y notificaciones	L2	L2
la identificación de componentes de infraestructura para su evaluación	L2	L2
la programación de evaluaciones de vulnerabilidad	L2	L2
la interpretación de resultados y la respuesta a éstos	L2	L2
el mantenimiento de un almacenamiento seguro y la disposición de datos sobre vulnerabilidad	L2	L2
[OP2.5.2] Los procedimientos de gestión de vulnerabilidades son objeto de seguimiento, así como de revisiones y actualizaciones periódicas.	L1	L2
[OP2.5.3] Las evaluaciones de vulnerabilidad de la tecnología se realizan de manera periódica, y las vulnerabilidades se tratan cuando se detectan.	L1	L3
[OP2.6] Codificación	L0	L3
[OP2.6.1] Se utilizan controles de seguridad apropiados para proteger la información sensible durante su almacenamiento o transmisión, incluidos	L0	L3
el cifrado de datos durante la transmisión	L2	L3
el cifrado de datos al escribir en disco	L0	L3
el uso de infraestructura de claves públicas	L0	L3
la tecnología de redes privadas virtuales	L2	L3
el cifrado de todas las transmisiones a través de Internet	L1	L3
[OP2.6.2] Se utilizan protocolos cifrados cuando se gestionan de manera remota sistemas, enrutadores y cortafuegos	L3	L3
[OP2.6.3] Los controles y protocolos de cifrado se someten a revisiones y comprobaciones periódicas	L1	L3
[OP2.7] Diseño y arquitectura de seguridad	L2	L2
[OP2.7.1] En la arquitectura y el diseño de sistemas nuevos y revisados se tienen en cuenta	L2	L2
las estrategias, políticas y procedimientos de seguridad	L2	L2
el historial de situaciones de riesgo en materia de seguridad	L2	L2
los resultados de las evaluaciones de riesgos para la seguridad	L2	L2
[OP2.7.2] La organización dispone de diagramas actualizados que muestren la tipología de red y la arquitectura de seguridad del conjunto de la empresa.	L3	L3

Comentarios:

[OP3] Seguridad del personal

salvaguarda	[presente]	[objetivo]
[OP3.1] Gestión de incidentes	L0	L3
[OP3.1.1] Existen procedimientos documentados para la identificación de presuntos incidentes e infracciones de seguridad, así como para la elaboración de informes al respecto, y para la adopción de respuestas a los mismos, entre los que figuran:	L1	L3
los incidentes que atañen a las redes	L1	L3
los incidentes relativos al acceso físico	L1	L3
los incidentes de ingeniería social	L1	L3
[OP3.1.2] Los procedimientos de gestión de incidentes se comprueban, verifican y actualizan periódicamente.	L1	L3
[OP3.1.3] Existen políticas y procedimientos documentados respecto a la colaboración con los órganos encargados de velar por el cumplimiento de las leyes.	L0	L3
[OP3.2] Prácticas de personal generales	L0	L2
[OP3.2.1]Los miembros del personal se atienen a buenas prácticas en materia de seguridad, como las que siguen:	L1	L2
asegurar la información respecto a la que son responsables	L2	L2
abstenerse de divulgar información sensible a terceros (resistencia a la ingeniería social)	L2	L2
disponer de la capacidad adecuada para utilizar los equipos y el software de las tecnologías de la información	L2	L2
utilizar buenas prácticas en lo que se refiere a las contraseñas	L1	L2
comprender y observar las políticas y reglamentos de seguridad	L3	L2
reconocer los incidentes e informar de éstos	L1	L2
[OP3.2.2] Todo el personal, a todas las escalas de responsabilidad, desempeña las funciones que se le han asignado y asume sus responsabilidades en lo que atañe a la seguridad de la información.	L2	L3
[OP3.2.3] Existen procedimientos documentados para autorizar y supervisar a aquéllos que manejan información sensible o trabajan en emplazamientos en los que se deposita la misma. Se trata de:	L0	L2
empleados	L2	L2
contratistas, socios, colaboradores, y personal de entidades terceras	L2	L2
personal de mantenimiento de sistemas	L2	L2
personal de mantenimiento de instalaciones	L0	L2

Comentarios:

Informe de Análisis de Riesgos 30.9.2008

(SME B)

Preparado:	GMV Soluciones Globales Internet		Clasification Type After Sanitization: UNCLASSIFIED
Verificado:	N/A	Código:	SGI-ERNSTING-INF-XXX
Aprobado:	Mª Teresa Avelino Carmona	Versión:	1
Autorizado:	Mª Teresa Avelino Carmona	Fecha:	30/09/2008

GMV SOLUCIONES GLOBALES INTERNET S.A.
P.T. Boecillo Parcela 101 - 47151 Valladolid.
Tel.: +34 983 54 65 54, Fax: +34 983 54 65 53.
www.gmv-sgi.es, www.gmv.com.

Código Interno: SGISA xxx/08

ESTA PÁGINA SE HA DEJADO EN BLANCO INTENCIONADAMENTE.

HOJA DE ESTADO DEL DOCUMENTO

Versión	Fecha	Págs.	Procesador	Cambios
1	15/09/2008	38	Word 2000 español	Primera versión

ÍNDICE

LISTA DE TABLAS Y FIGURAS

1. INTRODUCCIÓN

1.1. PROPÓSITO

El objeto del presente documento es plasmar los resultados obtenidos tras el análisis de riesgos realizado sobre los activos de información e instalaciones englobados en el alcance del mismo. Este análisis de riesgos se ha realizado dentro del ámbito de desarrollo del piloto de ENISA para la aplicación de su metodología adaptada a PYMES de análisis de riesgos, haciendo uso de la herramienta Pilar Basic 4.3 como apoyo para la aplicación de dicha metodología.

1.2. ALCANCE

El alcance del presente documento abarca las instalaciones y activos de información relativos a la actividad desarrollada en la sede de empresa B ubicada en X[1]

1.3. DEFINICIONES Y ACRÓNIMOS

1.3.1. DEFINICIONES

Concepto	Definición
Activo	Elementos del sistema de información que aportan valor a la organización
Confidencialidad	Garantía de que la información es accesible sólo a aquellas personas autorizadas a tener acceso a ella.
Disponibilidad	Garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.
Integridad	Garantía de que se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
Autenticación	Identificación de quién hace uso de los datos o servicios
Amenaza	Sucesos que pueden materializarse causando un perjuicio a la organización
Vulnerabilidad	Posibilidad de materialización de una amenaza sobre un activo
Riesgo	Índice que integra la probabilidad de que un escenario se materialice y la degradación que supondría sobre un activo
Impacto	Índice de daño o presión al que se ve sometido un servicio, proceso o activo en caso de la materialización de una amenaza
Salvaguardas	Elementos de defensa desplegados para reducir el perjuicio para la organización en caso de materialización de una amenaza

1.3.2. ACRÓNIMOS

Acrónimo	Concepto
[D]	Disponibilidad
[I]	Integridad
[C]	Confidencialidad
UE	Unión Europea

[1] SME name and location

2. REFERENCIAS

Los siguientes documentos son aplicables en la medida que tengan carácter contractual o hayan sido aprobados por el cliente, correspondiéndose sus versiones y fechas con las vigentes en el momento de publicación del presente documento; el resto se han usado simplemente a modo de soporte.

Código	Documento
[ENISA-INF]	Paquete informativo para PYME
[MAGERITV2]	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

3. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS[2]

Hoy en día nos encontramos en un entorno en el que la información se ha convertido en uno de los principales activos de cualquier organización. Se debe entender información en un sentido amplio, independientemente de la forma en la que se guarde o se transmita. Por lo tanto, esta información debe gestionarse y protegerse estratégicamente y de forma proactiva, incluyendo los sistemas y equipos o recursos que contribuyen a su almacenamiento, proceso y transmisión.

La gestión y protección de la información crítica de la organización deber realizarse de forma inteligente, identificando los procesos de negocio, los componentes que sustentan dichos procesos y las amenazas potenciales que podrían poner en peligro la normal ejecución de los mismos. Este esfuerzo de identificación y análisis debe facilitar la toma de decisiones en cuestión de seguridad, permitiendo priorizar las actuaciones que deben realizarse y optimizar el uso de los recursos. Esta tarea de análisis para la identificación de los puntos críticos de negocio y de las principales amenazas es una práctica que debe aplicarse de forma global y sistemática en el transcurso de la actividad diaria de la organización con el fin de invertir en seguridad de una forma racional, protegiendo aquellos activos que lo necesitan y con la intensidad necesaria.

Es aquí donde entra en juego el análisis de riesgos, que pretende sistematizar todo este proceso de análisis e identificación de actividades críticas para el negocio y amenazas potenciales con el fin de estimar la magnitud de los riesgos a los que está expuesta una organización. Esto permitirá conocer el estado actual de la organización en materia de seguridad, de forma que se pueda realizar una gestión adecuada de los riesgos identificados. Esta gestión de los riesgos consistirá en la planificación e implantación de las salvaguardas adecuadas de acuerdo a los objetivos, política y estrategia de la organización con el fin de reducir, transferir o asumir dichos riesgos. El riesgo no se puede erradicará totalmente, sino que el objetivo será reducirle a un nivel residual que sea asumible para la organización.

De forma general se puede dividir el proceso de análisis de riesgos en cuatro fases diferenciadas:

1. Identificación de activos relevantes para la organización. Entendiendo activo como cualquier recurso de información o relacionado con ésta necesario para la correcta ejecución de la actividad de la organización. Es obvio que no todos los activos son iguales, sino que pertenecerán a diferentes categorías (red, hardware, software, personas, etc.), lo cual condicionará las potenciales amenazas y las salvaguardas aplicables.
2. Identificación de amenazas. Amenazas son todos aquellos sucesos que pueden ocurrir y que puede causar un perjuicio a la organización. No todas las amenazas afectan a todos los activos, sino que hay una dependencia directa entre el tipo de activo y lo que le podría ocurrir. Así, podrían extorsionar a un empleado de la organización, mientras que no ocurre lo mismo con una aplicación o un servidor. De igual forma, no todos los activos se ven afectados de igual manera ni en el mismo grado por una determinada amenaza, por lo tanto es importante estimar cómo de vulnerable es un determinado activo atendiendo a dos aspectos:
    - Degradación: Cómo de perjudicado se vería el activo ante la materialización de la amenaza. Suele expresarse como un porcentaje del valor del activo.
    - Frecuencia: Cada cuanto es probable que se materialice la amenaza. Proporciona una nueva dimensión a la degradación que puede causar una amenaza, ya que una amenaza puede ser de terribles consecuencias pero de muy probable

[2] Here comes a short description about risk analysis process for an easier understanding of the report and the concepts used on it. a short explanation about the ENISA approach is also included in this section

materialización otra podría ser de muy bajas consecuencias pero tan frecuente como para acabar acumulando un daño considerable.

Mientras que estos dos aspectos nos determinan la forma en que una amenaza puede afectar un activo, es necesario determinar en qué sentido se puede producir este perjuicio. Para ello se pueden considerar tres dimensiones en las que un activo de información podría verse afectado:

- Disponibilidad: Se debe evaluar el perjuicio de que el activo no esté o no pueda ser utilizado.
- Confidencialidad: Se debe evaluar el perjuicio de que la información sea conocida por quien no debe.
- Integridad: Se debe valorar el perjuicio de que el activo o la información pueda estar manipulada, dañada o corrupta.

3. Identificación de salvaguardas existentes. Hasta este punto no se han tenido en cuenta las salvaguardas desplegadas, se tiene por lo tanto un mapa del riesgo potencial de la organización en el que se determinan los impactos y riesgos a que estarían expuestos los activos si no se protegieran, lo cual no es habitual. Las salvaguardas pueden tener dos efectos en el riesgo presente, bien reduciendo la frecuencia o la probabilidad de que una amenaza se materialice (salvaguardas preventivas) o bien limitando el impacto producido por una amenaza. Se puede considerar una salvaguarda efectiva al 100% cuando:

   - Es teóricamente idónea
   - Está perfectamente desplegada, configurada y mantenida
   - Se emplea siempre
   - Existen procedimientos claros de uso normal y en caso de incidencias
   - Los usuarios están formados y concienciados
   - Existen controles que avisan de posibles fallos

La forma en que se relacionan todos estos elementos se muestra en la siguiente figura:

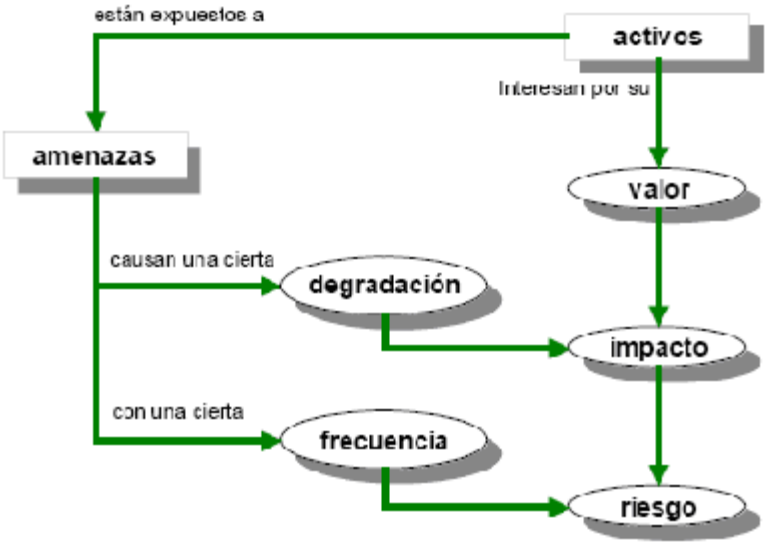

Figura 1: Relación de conceptos en el mapa de riesgos potencial

Una vez finalizado el análisis de riesgos se debe haber obtenido una visión de los impactos y riesgos residuales de la organización con las salvaguardas existentes. En el caso de que el riesgo residual no sea despreciable o asumible por la organización se tendrán que planificar y adoptar medidas que permitan alcanzar ese nivel de riesgo asumible para la organización. Es esto lo que se entiende por Gestión del Riesgo.

Durante el proceso de gestión del riesgo se deben seleccionar de forma prioritaria aquellas salvaguardas de tipo preventivo que permitan minimizar la probabilidad de que las amenazas se materialicen o que el daño producido sea despreciable. No obstante, dado que esto no es siempre posible, se deben adoptar en cualquier caso las medidas necesarias para que un posible incidente de seguridad no pase inadvertido, permitiendo su pronta detección, una reacción adecuada mediante un plan de emergencia y la posibilidad de recuperar el sistema a sus condiciones aceptables de funcionamiento lo antes posible mediante la elaboración de planes de continuidad.

Por último, debe tenerse en cuenta que una aplicación de salvaguardas eficiente debe llegar a un cierto equilibrio entre:

- Salvaguardas técnicas: en aplicaciones, equipos y comunicaciones
- Salvaguardas físicas: protegiendo el entorno de trabajo de las personas y los equipos
- Medidas de organización: de prevención y gestión de las incidencias
- Política de personal: siendo el factor humano el eslabón más débil de la seguridad, resulta de vital importancia contar con medidas adecuadas de contratación de personal, formación continua en buenas prácticas de seguridad, fomentar la participación en el reporte de incidencias y la aplicación de medidas disciplinarias cuando las normativas y política se seguridad de la organización se ven quebrantadas.

En cualquier caso se debe tener siempre presente que el punto óptimo vendrá dado por el equilibrio entre el valor del activo a proteger y la inversión realizada en salvaguardas para

protegerlo, considerando el valor del activo no sólo por su valor económico sino también en términos estratégicos, de reputación, etc.

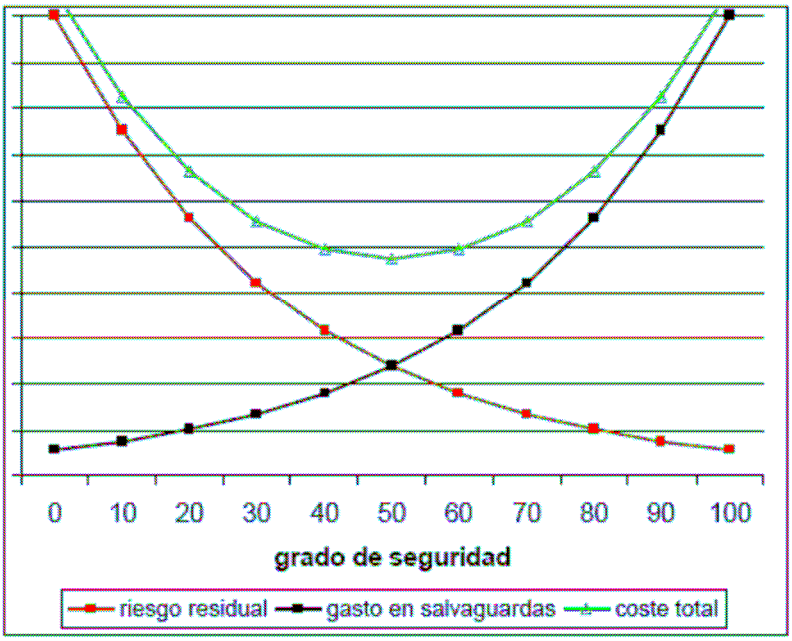

Figura 2: Grado de seguridad

En cuanto al proceso general de análisis de riesgos cabe destacar que existen diferentes metodologías que aportan diferentes enfoques a cada una de las diferentes fases que se pueden diferenciar, no obstante la mayor parte de ellas coinciden en la base conceptual y los objetivos, que han intentado plasmarse en el presente apartado.

El análisis de riesgos realizado dentro del ámbito de este piloto y cuyos resultados se expondrán en el presente documento se basa en la metodología desarrollada por ENISA. El principal objetivo de dicha metodología es la elaboración de un modelo simplificado de análisis de riesgos enfocado a pequeñas organizaciones que permita a dichas organizaciones realizar una evaluación del riesgo presente en sus entornos y seleccionar las medidas pertinentes para gestionar los riesgos identificados con un esfuerzo proporcional a sus recursos.

La metodología ENISA se basa en un enfoque en cuatro fases que tratan los siguientes aspectos:

1. Selección del perfil de riesgos: En esta fase se evalúa el perfil de riesgo de la organización mediante la utilización de un conjunto predefinido de criterios estructurados en una tabla de evaluación en la que la organización debe situarse.
2. Identificación de los activos críticos: En esta fase se seleccionan los activos más importantes en los procesos de negocio de la organización definiendo los requisitos de seguridad para cada uno de dichos activos y clasificándoles según su naturaleza.
3. Selección de tarjetas de controles o salvaguardas: Basándose en el perfil de riesgo de la organización y los requisitos de seguridad definidos para los activos de la empresa se seleccionan unos controles o salvaguardas aplicables.
4. Ejecución y gestión: Una vez determinados todos los aspectos anteriores y analizada la situación actual frente a la deseada se deben asignar prioridades en la ejecución de los controles.

Como herramienta de apoyo para aplicar la metodología se ha hecho uso de la aplicación Pilar Basic 4.3, resultado de la adaptación a la metodología ENISA de la herramienta EAR Pilar, ideada como herramienta de ayuda en la realización de los cálculos asociados al análisis de riesgos en sistemas complejos.

4. PERFIL DE RIESGO

La definición del perfil de riesgo según la metodología ENISA se realiza en base a la definición de la situación de la organización de acuerdo a las siguientes áreas y niveles:

Áreas de riesgo	Alto	Medio	Bajo
Riesgos jurídicos	La empresa maneja información de los clientes de carácter sensible y personal, incluidas historias médicas y datos personales críticos, con arreglo a lo previsto en la legislación de protección de datos de la UE	La empresa maneja la información de los clientes de índole personal, pero no sensible, conforme se define ésta en la Ley de protección de datos de la UE	La empresa no maneja datos personales distintos a los del personal empleado por ella
Riesgos de productividad	La empresa emplea a más de 100 personas que requieren a diario del acceso a aplicaciones y servicios empresariales	La empresa emplea a más de 50 personas que requieren a diario del acceso a aplicaciones y servicios empresariales	La empresa emplea a menos de 10 personas que requieren a diario del acceso a aplicaciones y servicios empresariales
Riesgos para la estabilidad financiera	Los ingresos anuales exceden de 25 millones de euros y/o las transacciones financieras con terceros o clientes tienen lugar como proceso habitual parte de su actividad empresarial	Los ingresos anuales no exceden de 25 millones de euros	Los ingresos anuales no exceden de 5 millones de euros
Riesgos para la reputación y de pérdida de confianza de los clientes	La indisponibilidad o la calidad del servicio repercuten directamente en el perfil empresarial, y/o más del 70% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa	La indisponibilidad o la calidad del servicio pueden repercutir indirectamente en el perfil empresarial, y/o menos del 5% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa	La indisponibilidad o la calidad del servicio no pueden repercutir de manera directa o indirecta en el perfil empresarial, ni derivar en pérdida de ingresos

Tabla 1: Criterios de definición del perfil de riesgos

En el caso que nos ocupa, la empresa B centra su actividad en XXXX[3]

[3] Here there come the comments over the reasons why we chose the risk profile based on the table about and the answers made to questions in the questionnaire and another one regarded with the SME business environment

Por lo tanto de acuerdo a las características de la empresa analizada y en base a los criterios definidos en la metodología ENISA de análisis de riesgos y según la percepción de la propia empresa, se pueden determinar los niveles de riesgo que se muestran en la siguiente tabla, siendo el valor más alto y el que determina el perfil de riesgo global de la empresa "**Medio**"[4]

Áreas de riesgo	Nivel de riesgo	Perfil de Riesgo
Riesgos jurídicos (*Legal and Regulatory*)	Medio (*Medium*)	Alto *(High)*
Riesgos de productividad (*Productivity*)	Medio (*Medium*)	
Riesgos para la estabilidad financiera (*Financial Stability*)	Medio (*Medium*)	
Riesgos para la reputación y de pérdida de confianza de los clientes (*Reputation and Loss of Customer Confidence*)	Alto *(High)*	

Tabla 2: Perfil de riesgo de la empresa

[4] Risk profile selection for each defined risk area

5. ACTIVOS CRÍTICOS

Tal y como se ha explicado en el apartado anterior, se han identificado dos actividades críticas para la empresa B[5]:

- XXXXXXXX
- XXXXXXXX

De forma adicional se puede destacar que la empresa dispone de portal web y servicio de correo electrónico en régimen de hosting.

Teniendo en cuenta los datos anteriores y la entrevista mantenida con los responsables de la empresa se han identificado y clasificado los siguientes activos críticos que serán incluidos en el análisis de riesgos:[6]

- Aplicaciones (*Applications*):
  - [Financial Control]
  - [CRM]
- Equipos (*Systems*)
  - [Web Server]
  - [Archiving and Backup Server, BBDD]
  - [Mail Server]
  - [workstations]
- Comunicaciones (*Network*)
  - [Cabling, routers and network segments]
  - [PABX]
  - [telephones]
- Personal (*People*)
  - [Operation and technology]
  - [Sales and marketing]
  - [Administrative assistants and human resources management]

De acuerdo a la metodología ENISA los activos enumerados pueden englobarse dentro de las siguientes categorías:[7]

[5] Critical Business activities identification

[6] Assets identification

[7] Assets categorization and security requirements identification

Activo crítico (Critical Asset)	Categoría de activo (*Asset category*)	Componentes (*Components*)	Requisitos de seguridad (*Security requirements*)	Justificación de su selección (*Justification*)
Portal web (*web portal*)	Aplicación (*Application*)	Todos los activos definidos en este apartado	Integridad (Integrity) Disponibilidad (Availability)	XXXXX

Tabla 3: Activos seleccionados

6. SELECCIÓN DE CONTROLES

La metodología ENISA define una serie de salvaguardas organizativas y orientadas a activos que deben seleccionarse o que son recomendables según el perfil de riesgo de la empresa y los activos críticos de la misma.

Según el perfil de riesgo definido para cada una de las áreas y teniendo en cuenta las especificaciones de la metodología ENISA se pueden seleccionar los siguientes controles:[8]

Áreas de riesgo (*Risk areas*)	Nivel de riesgo (*Risk level*)	Controles organizativos (*Organizational controls*)
Riesgos jurídicos (*Legal and Regulatory*)	Medio (*Medium*)	SP1 SP4
Riesgos de productividad (*Productivity*)	Medio (*Medium*)	SP4 SP6
Riesgos para la estabilidad financiera (*Financial Stability*)	Medio (*Medium*)	SP4
Riesgos para la reputación y de pérdida de confianza de los clientes (*Reputation and Loss of Customer Confidence*)	Alto *(High)*	SP1 SP5

Tabla 4: Salvaguardas organizativas recomendadas

[8] Organizational controls

Basándonos en el perfil de riesgos global y la categorización de los activos, según la metodología ENISA se deben seleccionar los controles pertenecientes al grupo CC-2S que agrupa las siguientes salvaguardas:[9]

Identificación de la tarjeta de controles basados en los activos (*Asset Bases Control card ID*)										
							CC-1A			
Perfil de riesgos (*Risk profile*)							Alto			
Categoría del activo (*Asset category*)							Aplicación			
Requisitos de seguridad (*Security requirements*)	Seguridad Física (*Physical Security*)	Gestión de sistemas y redes (*System and network Management*)	Herramientas de administración de sistemas (*System Administration tools*)	Seguimiento y auditoría de la seguridad física (*Monitoring and Auditing IT Security*)	Autenticación y autorización (*Authenticatioon and Authorization*)	Gestión de vulnerabilidades (*Vulnerability Management*)	Cifrado (*Encryption*)	Diseño y arquitectura de seguridad (*Securioty Architecture and Design*)	Gestión de incidentes (*Incident Management*)	Prácticas de personal generales (*General Staff practices*)
Confidencialidad (*Condifentiality*)		OP2.1.3			OP2.4.2	OP2.5.1	OP2.6.1			
Integridad (*Integrity*)		OP2.1.4			OP2.4.2	OP2.5.1	OP2.6.1			
Disponibilidad (*Availability*)		OP2.1.6								

Tabla 5: Salvaguardas orientada a activos recomendadas

[9] Score card selection and asset based controls

De esta forma se pueden concluir los siguientes controles a implantar en el sistema:

Activo	Control	Justificación de su selección
Controles basados en los activos	OP2.1.4 OP2.1.6 OP2.4.2 OP2.5.1 OP2.6.1	Los controles de autenticación y autorización, así como los de gestión de red son esenciales para mantener la disponibilidad y confidencialidad del activo objeto en consideración
Controles organizativos	SP1	Formación y sensibilización en materia de seguridad
	SP4	Política de seguridad
	SP5	Gestión de la seguridad con terceros
	SP6	Planificación de contingencias

Tabla 6: Salvaguardas recomendadas

En los siguientes aparatados del presente documento se profundiza en los aspectos incluidos en cada una de los controles recomendados, así como en el análisis entre el estado actual de implantación y el nivel recomendado de los mismos.

7. ANÁLISIS DEL ESTADO ACTUAL VS OBJETIVO

Con el objetivo de realizar una gestión y priorización adecuada de los controles seleccionados, se debe realizar un análisis que nos permita contrastar el estado actual de aplicación de las diferentes salvaguardas en la organización respecto el estado recomendable de las mismas. Para facilitar la realización de este análisis se ha dividido el grado de implantación de las salvaguardas según los siguientes niveles[10]:

- L0. La salvaguarda no se encuentra implantada en la organización.
- L1. En este nivel de madurez, las salvaguardas existen, pero no se gestionan. El éxito depende de buena suerte. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta.
- L2. En este nivel de madurez, la eficacia de las salvaguardas depende de la buena suerte y de la buena voluntad de las personas. Los éxitos son repetibles, pero no hay plan para los incidentes más allá de la reacción heroica. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.
- L3. Se despliegan y se gestionan las salvaguardas. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular de las protecciones. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece.
- L4. Usando medidas de campo, la dirección puede controlar empíricamente la eficacia y la efectividad de las salvaguardas. En particular, la dirección puede fijar metas cuantitativas de la calidad. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa, mientras que en el nivel L3, la confianza era solamente cualitativa.
- L5. Este nivel de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora de los procesos. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.

De esta forma, en las siguientes tablas se plasma para cada una de los grupos de salvaguarda la comparativa entre el estado actual y el estado objetivo o recomendable según el modelado de la metodología ENISA realizado mediante la herramienta Pilar. Las valoraciones asignadas a cada una de las salvaguardas tanto para el estado actual como el objetivo son fruto de la entrevista mantenida con la empresa y la experiencia de la empresa GMV en la realización de análisis de riesgos.

[10] Here comes by safeguard, the tables with the current situation and the regarded situation as ENISA suggests. we have done a gap analysis considering the current situation based on the meeting held with the SME. the maturity level for each control has been evaluated in six levels l0-l5 in order to simplify the gap analysis.

For each table with the safeguards and the evaluation, we have made comments with the justification or any finding that echoes the evidence if required.

[SP1] Formación y sensibilización en materia de seguridad

Salvaguarda	[presente]	[objetivo]
[SP1.1] Los miembros del personal comprenden sus funciones y responsabilidades en materia de seguridad. Este hecho está documentado y comprobado.	L2	L4
[SP1.2] Se dispone de conocimientos técnicos internos adecuados para la totalidad de servicios, mecanismos y tecnologías empleados (p. Ej., registro, seguimiento o codificación), incluido el funcionamiento de éstos en condiciones de seguridad. Este hecho está documentado y comprobado.	L2	L4
[SP1.3] Se imparten a todo el personal conocimientos y formación y se le envían recordatorios periódicos en materia de seguridad. El conocimiento del personal está documentado, y la conformidad se comprueba periódicamente. La formación comprende los temas que siguen:	L0	L3
estrategias, metas y objetivos en materia de seguridad	L1	L3
reglamentos, políticas y procedimientos de seguridad	L0	L3
políticas y procedimientos de colaboración con terceros	L1	L3
planes para contingencias y recuperación en caso de catástrofe	L1	L3
requisitos relativos a la seguridad física	L1	L3
perspectiva de los usuarios respecto a	L1	L3
la gestión de sistemas y redes	L1	L3
las herramientas de administración del sistema	L1	L3
el seguimiento y la auditoría en lo que atañe a la seguridad física y asociada a las tecnologías de la información	L1	L3
autenticación y autorización	L1	L3
gestión de vulnerabilidades	L0	L3
Codificación	L0	L3
arquitectura y diseño	L0	L3
gestión de incidentes	L0	L3
prácticas generales de personal	L1	L3
observancia de la legislación, sanciones y actuaciones disciplinarias por infracciones de la seguridad	L1	L3
modo de acceder correctamente a la información sensible y trabajo en las áreas en las que ésta es accesible	L1	L3
políticas y procedimientos de extinción de la relación laboral en lo que atañe a la seguridad	L2	L3

Comentarios:[11]

[11] Regarded comments. Example: Staff members apply common security practices based on their own knowledge. These practices are not documented or linked with internal policy or employee's contracts.

Organization common security practices should be documented and included in the internal training program. In addition, staff members should sign non disclosure agreements at the beginning of working relationship. …

[SP4] Políticas y normativas de seguridad

salvaguarda	[presente]	[objetivo]
[SP4.1] La organización dispone de un conjunto exhaustivo de políticas vigentes y documentadas que se revisan y actualizan periódicamente. Estas políticas abordan áreas temáticas fundamentales en materia de seguridad, entre las que se cuentan:	L1	L2
la gestión y la estrategia de seguridad	L1	L2
la gestión de riesgos para la seguridad	L1	L2
la seguridad física	L1	L2
la gestión de sistemas y redes	L2	L2
las herramientas de administración de sistemas	L1	L2
el seguimiento y la auditoría	L1	L2
la autenticación y la autorización	L2	L2
la gestión de vulnerabilidades	L1	L2
la codificación	L1	L2
la arquitectura y el diseño de la seguridad	L1	L2
la gestión de incidentes	L1	L2
las prácticas de seguridad de personal	L1	L2
la legislación aplicable	L3	L2
la sensibilización y la formación	L1	L2
la seguridad de la información basada en la colaboración	L1	L2
la planificación de contingencias y la recuperación en caso de catástrofe	L2	L2
[SP4.2] Existe un proceso documentado para la gestión de políticas de seguridad, incluidas las tareas de:	L1	L2
creación	L1	L2
administración (incluidas revisiones y actualizaciones periódicas)	L1	L2
comunicación	L1	L2
[SP4.3] La organización cuenta con un proceso documentado para la evaluación periódica (técnica y no técnica) del cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L1	L4
[SP4.4] La organización cuenta con un proceso documentado para garantizar el cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L1	L4
[SP4.5] La organización aplica de manera uniforme sus políticas de seguridad.	L1	L4
[SP4.6] Únicamente el personal autorizado puede comprobar y revisar las políticas y procedimientos de seguridad.	L2	L4

Comentarios:

[SP5] Gestión de la seguridad en régimen de colaboración

Salvaguarda	[presente]	[objetivo]
[SP5.1] La organización ha procedido a la documentación, el seguimiento y la ejecución de procedimientos para la protección de su información cuando colabora con entidades externas (p. Ej., terceros, colaboradores, subcontratistas o socios).	L1	L3
[SP5.2] La organización ha comprobado que los servicios, mecanismos y tecnologías de seguridad externalizados satisfacen sus necesidades y requisitos.	L2	L3
[SP5.3] La organización documenta, supervisa y aplica estrategias de protección de la información perteneciente a entidades externas a la que se accede desde componentes de su infraestructura, o que es utilizada por su personal.	n.a.	n.a.
[SP5.4] La organización ofrece y verifica actividades de sensibilización y formación sobre las políticas y los procedimientos de seguridad de entidades externas para el personal que interactúa con éstas.	n.a.	n.a.
[SP5.5] Existen procedimientos documentados respecto al personal externo cuya relación con la organización ha concluido, en los que se especifican las medidas de seguridad pertinentes para finalizar su posibilidad de acceso. Estos procedimientos se comunican a la organización externa y se coordinan con ella.	n.a.	n.a.

Comentarios

[SP6] Planificación de contingencias / recuperación en caso de catástrofe

salvaguarda	[presente]	[objetivo]
[SP6.1] Se ha efectuado un análisis de operaciones, aplicaciones y de la significación de los datos.	L2	L3
[SP6.2] La organización ha documentado	L2	L3
los planes de continuidad de la actividad empresarial y de operación en casos de emergencia	L2	L3
los planes de recuperación en caso de catástrofe	L2	L3
los planes de contingencia para la respuesta en casos de emergencia	L2	L3
[SP6.3] En los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial se consideran los requisitos y controles de acceso físico y electrónico.	L2	L3
[SP6.4] Los planes de contingencia, recuperación en caso de catástrofe, y continuidad de la actividad empresarial se revisan y comprueban periódicamente.	L1	L3
[SP6.5] Todo el personal ...	L1	L2
tiene conocimiento de los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial	L1	L2
comprende sus responsabilidades y está capacitado para cumplirlas	L1	L2

Comentarios

[OP2] Seguridad de las tecnologías de la información

salvaguarda	[presente]	[objetivo]
[OP2.1.4] La integridad del software instalado se verifica regularmente.	L3	L4
[OP2.1.6] Existe un plan de copias de respaldo de datos que	L2	L3
se actualiza regularmente	L2	L3
se comprueba periódicamente	L2	L3
requiere la realización de copias de respaldo programadas	L2	L3

regularmente, tanto del software, como de los datos		
requiere la comprobación y verificación periódicas de la capacidad para restaurar a partir de copias de respaldo	L2	L3
[OP2.4.2] Existen políticas y procedimientos de uso de la información documentados respecto al acceso individual y en grupo con el fin de:	L2	L3
establecer las normas de concesión del nivel pertinente de acceso	L2	L3
establecer un derecho inicial de acceso	L2	L3
modificar el derecho de acceso	L2	L3
anular el derecho de acceso	L2	L3
revisar y comprobar periódicamente los derechos de acceso	L2	L3
[OP2.5.1] Existe un conjunto documentado de procedimientos para la gestión de vulnerabilidades, entre los que figuran:	L1	L2
la selección de herramientas de evaluación de vulnerabilidades, listas de comprobación y scripts	L1	L2
el mantenimiento al día respecto a los tipos de vulnerabilidades conocidos y los métodos de ataque	L1	L2
la revisión de fuentes de información sobre anuncios de vulnerabilidad, alertas de seguridad y notificaciones	L1	L2
la identificación de componentes de infraestructura para su evaluación	L1	L2
la programación de evaluaciones de vulnerabilidad	L1	L2
la interpretación de resultados y la respuesta a éstos	L1	L2
el mantenimiento de un almacenamiento seguro y la disposición de datos sobre vulnerabilidad	L1	L2
[OP2.6.1] Se utilizan controles de seguridad apropiados para proteger la información sensible durante su almacenamiento o transmisión, incluidos	L0	L3
el cifrado de datos durante la transmisión	L0	L3
el cifrado de datos al escribir en disco	L0	L3
el uso de infraestructura de claves públicas	L0	L3
la tecnología de redes privadas virtuales	L0	L3
el cifrado de todas las transmisiones a través de Internet	L1	L3

Comentarios

8. RESUMEN EJECUTIVO

XXXXX[12]

[12] Here comes the most important aspects and recommendations that the SME should take into account with regard to ENISA risk analysis approach and GMV expertise. it includes recommendations about the selected scorecards in ENISA methodology and other relevant aspects

9. ANEXO A: RESULTADOS DE LA HERRAMIENTA PILAR

La herramienta Pilar permite completar los resultados de la metodología ENISA con consideraciones más específicas de análisis de riesgos, enriqueciendo los resultados obtenidos con datos más específicos y gráficos que permiten contrastar de forma rápida y sencilla la evolución del riesgo en la organización respecto al grado de implantación de las salvaguardas.

En cuanto a la selección de amenazas, la herramienta Pilar permite definir las amenazas de interés para cada uno de los activos. Cada una de estas amenazas tendrá asociados unos parámetros de impacto para cada una de las dimensiones de seguridad en caso de materialización y frecuencia de ocurrencia. En la versión utilizada de la herramienta para el desarrollo del piloto, se seleccionan unas amenazas por defecto para cada tipo de activo según su naturaleza, personas, red, hardware, ..., con valores también por defecto para la frecuencia y el impacto. Esto permite al usuario abstraerse de la complejidad asociada a la selección de este tipo de parámetros durante el análisis de riesgos a la vez que se permite desglosar la información del mapa de riesgo por cada una de las amenazas asociadas a los activos. De forma complementaria a las amenazas seleccionadas por defecto la herramienta permite seleccionar amenazas adicionales que permitan adaptarse a los diferentes requisitos del sector de actividad de cada empresa. Las amenazas por defecto para cada uno de los activos que han sido seleccionadas en la herramienta son las siguientes:

Aplicaciones
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.19] Escapes de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.14] Interceptación de información (escucha)
[A.22] Manipulación de programas

Tabla 7: Amenazas de aplicaciones

Equipos
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico

[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.19] Escapes de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.14] Interceptación de información (escucha)
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo

Tabla 8: Amenazas de equipos

Comunicaciones
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia

[E.19] Escapes de información
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.14] Interceptación de información (escucha)
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo

Tabla 9: Amenazas de comunicaciones

Personas
[E.7] Deficiencias en la organización
[E.19] Escapes de información
[E.28] Indisponibilidad del personal
[A.19] Divulgación de información
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)

Tabla 10: Amenazas de personas

En cuanto al mapa de riesgos, la herramienta permite representar de forma gráfica el riesgo presente en la organización en diferentes momentos en función del estado de implantación de las salvaguardas en dichos momentos. En el desarrollo del piloto se han analizado las siguientes estados:[13]

- Riesgo potencial: Riesgo en caso de no existir implantada ninguna salvaguarda.
- Riesgo presente: Riesgo existente en la organización con el estado de implantación actual de las salvaguardas.
- Riesgo objetivo: Riesgo existente en la organización si se implantasen las salvaguardas recomendadas por la metodología ENISA y aquellas recomendaciones fruto de la experiencia de la empresa GMV y los aspectos analizados durante las entrevistas mantenidas con la empresa.

Cada uno de estos mapas de riesgo pueden observarse en las siguientes figuras.

[13] Here comes the potential risk, current risk and target risk images obtained from PILAR tool for each SME.

activo	[D]	[I]	[C]
ACTIVOS	{8.3}	{8.3}	{8.3}
[SW] Aplicaciones	{7.9}	{8.3}	{8.3}
[ ]	{7.9}	{8.3}	{8.3}
[ ]	{7.9}	{8.3}	{8.3}
[HW] Equipos	{8.3}	{8.3}	{8.3}
[ ]	{8.3}	{8.3}	{8.3}
[ ]	{8.3}	{8.3}	{8.3}
[ ]	{8.3}	{8.3}	{8.3}
[ ]	{8.3}	{8.3}	{8.3}
[COM] Comunicaciones	{7.9}	{5.3}	{7.3}
[ ]	{7.6}	{5.3}	{7.3}
[ ]	{7.9}	{5.3}	{7.3}
[ ]	{7.6}	{5.3}	{7.3}
[P] Personal	{6.3}	{6.9}	{7.0}
[ ]	{6.0}	{5.5}	{5.6}
[ ]	{6.0}	{5.5}	{5.6}
[ ]	{6.3}	{6.9}	{7.0}

Figura 3: Riesgo potencial

activo	[D]	[I]	[C]
ACTIVOS	{6.0}	{6.1}	{6.1}
[SW] Aplicaciones	{5.8}	{6.1}	{6.1}
[ ]	{5.8}	{6.1}	{6.1}
[ ]	{5.8}	{6.1}	{6.1}
[HW] Equipos	{6.0}	{5.9}	{5.9}
[ ]	{6.0}	{5.9}	{5.9}
[ ]	{6.0}	{5.9}	{5.9}
[ ]	{6.0}	{5.9}	{5.9}
[ ]	{6.0}	{5.9}	{5.9}
[COM] Comunicaciones	{5.8}	{3.0}	{5.3}
[ ]	{5.5}	{3.0}	{5.3}
[ ]	{5.8}	{3.0}	{5.2}
[ ]	{5.5}	{3.0}	{5.3}
[P] Personal	{4.2}	{4.8}	{4.9}
[ ]	{4.0}	{3.4}	{3.5}
[ ]	{4.0}	{3.4}	{3.5}
[ ]	{4.2}	{4.8}	{4.9}

Figura 4: Riesgo Presente

activo	[D]	[I]	[C]
ACTIVOS	{3.5}	{3.5}	{3.6}
[SW] Aplicaciones	{3.3}	{3.5}	{3.6}
[ ]	{3.3}	{3.5}	{3.6}
[ ]	{3.3}	{3.5}	{3.6}
[HW] Equipos	{3.5}	{3.4}	{3.4}
[ ]	{3.5}	{3.4}	{3.4}
[ ]	{3.5}	{3.4}	{3.4}
[ ]	{3.5}	{3.4}	{3.4}
[ ]	{3.5}	{3.4}	{3.4}
[COM] Comunicaciones	{3.2}	{0.4}	{2.5}
[ ]	{2.9}	{0.4}	{2.5}
[ ]	{3.2}	{0.4}	{2.4}
[ ]	{2.9}	{0.4}	{2.5}
[P] Personal	{1.8}	{2.4}	{2.5}
[ ]	{1.5}	{1.0}	{1.0}
[ ]	{1.5}	{1.0}	{1.0}
[ ]	{1.8}	{2.4}	{2.5}

Figura 5: Riesgo objetivo

En el proyecto de la herramienta Pilar proporcionado a la empresa se pueden desglosar cada uno de los mapas de riesgo anteriores en función de las distintas amenazas.

Adicionalmente, el análisis completo de implantación de salvaguardas que se ha tenido en cuenta para la obtención de los mapas de riesgo anteriores se presenta en el Anexo B del presente documento.

10. ANEXO B: ESTADO DE IMPLANTACIÓN DE SALVAGUARDAS[14]

[SP1] Formación y sensibilización en materia de seguridad

Salvaguarda	[presente]	[objetivo]
[SP1.1] Los miembros del personal comprenden sus funciones y responsabilidades en materia de seguridad. Este hecho está documentado y comprobado.	L2	L4
[SP1.2] Se dispone de conocimientos técnicos internos adecuados para la totalidad de servicios, mecanismos y tecnologías empleados (p. Ej., registro, seguimiento o codificación), incluido el funcionamiento de éstos en condiciones de seguridad. Este hecho está documentado y comprobado.	L2	L4
[SP1.3] Se imparten a todo el personal conocimientos y formación y se le envían recordatorios periódicos en materia de seguridad. El conocimiento del personal está documentado, y la conformidad se comprueba periódicamente. La formación comprende los temas que siguen:	L0	L3
estrategias, metas y objetivos en materia de seguridad	L1	L3
reglamentos, políticas y procedimientos de seguridad	L0	L3
políticas y procedimientos de colaboración con terceros	L1	L3
planes para contingencias y recuperación en caso de catástrofe	L1	L3
requisitos relativos a la seguridad física	L1	L3
perspectiva de los usuarios respecto a	L1	L3
la gestión de sistemas y redes	L1	L3
las herramientas de administración del sistema	L1	L3
el seguimiento y la auditoría en lo que atañe a la seguridad física y asociada a las tecnologías de la información	L1	L3
autenticación y autorización	L1	L3
gestión de vulnerabilidades	L0	L3
Codificación	L0	L3
arquitectura y diseño	L0	L3
gestión de incidentes	L0	L3
prácticas generales de personal	L1	L3
observancia de la legislación, sanciones y actuaciones disciplinarias por infracciones de la seguridad	L1	L3
modo de acceder correctamente a la información sensible y trabajo en las áreas en las que ésta es accesible	L1	L3
políticas y procedimientos de extinción de la relación laboral en lo que atañe a la seguridad	L2	L3

Comentarios

[SP2] Estrategia de seguridad

[14] Here comes by safeguard, the tables with the current situation and the target situation. in this section, we have included the gap analysis for safeguards not suggested by ENISA approach but GMV consider that are important controls to take into account by the SME.

salvaguarda	[presente]	[objetivo]
[SP2.1] Las estrategias empresariales de la organización incorporan de manera rutinaria consideraciones de seguridad.	L2	L2
[SP2.2] En las estrategias y políticas de seguridad se tienen en cuenta las estrategias y objetivos empresariales de la organización.	L2	L2
[SP2.3] Las estrategias, metas y objetivos en materia de seguridad se documentan y se revisan, actualizan y comunican periódicamente a la organización.	L2	L2

[SP3] Gestión de seguridad

salvaguarda	[presente]	[objetivo]
[SP3.1] La dirección asigna fondos y recursos suficientes a las actividades de seguridad de la información.	L1	L1
[SP3.2] Se definen funciones y responsabilidades en materia de seguridad para todo el personal de la organización.	L2	L2
[SP3.3] En las prácticas de la organización en materia de contratación y de extinción de la relación laboral con el personal se tienen en cuenta las cuestiones de seguridad de la información.	L2	L2
[SP3.4] Los niveles requeridos de seguridad de la información y el modo en que se aplican a personas y grupos se documentan y aplican.	L2	L2
[SP3.5] La organización gestiona los riesgos que atañen a la seguridad de la información, con inclusión de:	L1	L1
la evaluación de los riesgos para la seguridad de la información, tanto periódicamente, como en respuesta a cambios significativos en la tecnología, amenazas internas o externas, o los sistemas y operaciones de la organización	L1	L1
la adopción de medidas para mitigar los riesgos hasta alcanzar un nivel aceptable	L1	L1
el mantenimiento de un nivel de riesgos aceptable	L1	L1
la utilización de evaluaciones de riesgos para la seguridad de la información con el fin de facilitar la selección de medidas de seguridad y control rentables, equilibrando los costes de ejecución con las posibles pérdidas	L1	L1
[SP3.6] La dirección recibe informes rutinarios, y actúa basándose en ellos, en los que se resumen los resultados de:	L1	L1
la revisión de los registros de sistema	L1	L1
la revisión de los historiales de auditoría	L1	L1
las evaluaciones de vulnerabilidades tecnológicas	L1	L1
los incidentes de seguridad y las respuestas dadas a los mismos	L1	L1
las evaluaciones de riesgos	L1	L1
las revisiones de la seguridad física	L1	L1
los planes y recomendaciones para la mejora de la seguridad	L1	L1

[SP4] Políticas y normativas de seguridad

salvaguarda	[presente]	[objetivo]
[SP4.1] La organización dispone de un conjunto exhaustivo de políticas vigentes y documentadas que se revisan y actualizan periódicamente. Estas políticas abordan áreas temáticas fundamentales en materia de seguridad, entre las que se cuentan:	L1	L2
la gestión y la estrategia de seguridad	L1	L2
la gestión de riesgos para la seguridad	L1	L2
la seguridad física	L1	L2

la gestión de sistemas y redes	L2	L2
las herramientas de administración de sistemas	L1	L2
el seguimiento y la auditoría	L1	L2
la autenticación y la autorización	L2	L2
la gestión de vulnerabilidades	L1	L2
la codificación	L1	L2
la arquitectura y el diseño de la seguridad	L1	L2
la gestión de incidentes	L1	L2
las prácticas de seguridad de personal	L1	L2
la legislación aplicable	L3	L2
la sensibilización y la formación	L1	L2
la seguridad de la información basada en la colaboración	L1	L2
la planificación de contingencias y la recuperación en caso de catástrofe	L2	L2
[SP4.2] Existe un proceso documentado para la gestión de políticas de seguridad, incluidas las tareas de:	L1	L2
creación	L1	L2
administración (incluidas revisiones y actualizaciones periódicas)	L1	L2
comunicación	L1	L2
[SP4.3] La organización cuenta con un proceso documentado para la evaluación periódica (técnica y no técnica) del cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L1	L4
[SP4.4] La organización cuenta con un proceso documentado para garantizar el cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L1	L4
[SP4.5] La organización aplica de manera uniforme sus políticas de seguridad.	L1	L4
[SP4.6] Únicamente el personal autorizado puede comprobar y revisar las políticas y procedimientos de seguridad.	L2	L4

Comentarios

[SP5] Gestión de la seguridad en régimen de colaboración

Salvaguarda	[presente]	[objetivo]
[SP5.1] La organización ha procedido a la documentación, el seguimiento y la ejecución de procedimientos para la protección de su información cuando colabora con entidades externas (p. Ej., terceros, colaboradores, subcontratistas o socios).	L1	L3
[SP5.2] La organización ha comprobado que los servicios, mecanismos y tecnologías de seguridad externalizados satisfacen sus necesidades y requisitos.	L2	L3
[SP5.3] La organización documenta, supervisa y aplica estrategias de protección de la información perteneciente a entidades externas a la que se accede desde componentes de su infraestructura, o que es utilizada por su personal.	n.a.	n.a.
[SP5.4] La organización ofrece y verifica actividades de sensibilización y formación sobre las políticas y los procedimientos de seguridad de entidades externas para el personal que interactúa con éstas.	n.a.	n.a.
[SP5.5] Existen procedimientos documentados respecto al personal externo cuya relación con la organización ha concluido, en los que se especifican las medidas de seguridad pertinentes para finalizar su	n.a.	n.a.

posibilidad de acceso. Estos procedimientos se comunican a la organización externa y se coordinan con ella.		

Comentarios

[SP6] Planificación de contingencias / recuperación en caso de catástrofe

salvaguarda	[presente]	[objetivo]
[SP6.1] Se ha efectuado un análisis de operaciones, aplicaciones y de la significación de los datos.	L2	L3
[SP6.2] La organización ha documentado	L2	L3
los planes de continuidad de la actividad empresarial y de operación en casos de emergencia	L2	L3
los planes de recuperación en caso de catástrofe	L2	L3
los planes de contingencia para la respuesta en casos de emergencia	L2	L3
[SP6.3] En los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial se consideran los requisitos y controles de acceso físico y electrónico.	L2	L3
[SP6.4] Los planes de contingencia, recuperación en caso de catástrofe, y continuidad de la actividad empresarial se revisan y comprueban periódicamente.	L1	L3
[SP6.5] Todo el personal ...	L1	L2
tiene conocimiento de los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial	L1	L2
comprende sus responsabilidades y está capacitado para cumplirlas	L1	L2

Comentarios

[OP1] Seguridad física

salvaguarda	[presente]	[objetivo]
[OP1.1] Planes y procedimientos de seguridad física	L1	L2
[OP1.1.1] Existen planes de seguridad de las instalaciones documentados, concebidos para salvaguardar locales, edificios y cualquier otra área restringida.	L2	L2
[OP1.1.2] Estos planes se revisan, comprueban y actualizan periódicamente.	L1	L2
[OP1.1.3] Los procedimientos y mecanismos de seguridad física se comprueban y revisan periódicamente.	L1	L2
[OP1.1.4] Existen políticas y procedimientos documentados para la gestión de visitantes, que incluyen	L1	L2
el registro en la entrada	L1	L2
el acompañamiento por las instalaciones	L1	L2
los registros de acceso	L1	L2
la recepción y los servicios de hospitalidad	L1	L2
[OP1.1.5] Existen políticas y procedimientos documentados para el control físico del hardware y el software, incluidos	L1	L2
terminales, portátiles, módem, componentes inalámbricos y todos los demás elementos utilizados para acceder a la información	L2	L2
el acceso, el almacenamiento y la recuperación de copias de seguridad de datos	L2	L2
el almacenamiento de información sensible en medios físicos y electrónicos	L2	L2
la supresión de información sensible, o de los medios en los que se encuentra almacenada	L1	L2

la reutilización y el reciclaje de papel y medios electrónicos.	L1	L2
[OP1.2] Control de acceso físico	L2	L3
[OP1.2.1] Existen políticas y procedimientos documentados respecto al acceso individual y en grupo, que comprenden:	L2	L3
las normas de concesión del nivel pertinente de acceso físico	L2	L3
las normas para la determinación de los derechos iniciales de acceso	L2	L3
la modificación del derecho de acceso	L2	L3
la anulación del derecho de acceso	L2	L3
la revisión y la comprobación periódicas de los derechos de acceso	L2	L3
[OP1.2.2] Existen políticas, procedimientos y mecanismos documentados para controlar el acceso físico a entidades definidas. Se incluyen aquí:	L2	L3
áreas de trabajo	L2	L3
medios de hardware (ordenadores, dispositivos de comunicación, etc.) y de software	L2	L3
[OP1.2.3] Existen procedimientos documentados para verificar la autorización de acceso antes de autorizar el acceso físico.	L2	L3
[OP1.2.4] Los terminales y otros componentes que permiten el acceso a información sensible se encuentran físicamente protegidos con el fin de evitar accesos no autorizados.	L3	L3
[OP1.3] Seguimiento y auditoría de la seguridad física	L1	L3
[OP1.3.1] Se conservan registros de mantenimiento para documentar las reparaciones y modificaciones de los componentes físicos de las instalaciones.	L1	L3
[OP1.3.2] Pueden justificarse las acciones de una persona o de un grupo respecto a la totalidad de medios controlados físicamente.	L1	L4
[OP1.3.3] Se examinan regularmente registros de auditoría y seguimiento para detectar anomalías, y se emprenden acciones correctivas en caso necesario.	L1	L3

Comentarios

[OP2] Seguridad de las tecnologías de la información

salvaguarda	[presente]	[objetivo]
[OP2.1] Gestión de sistemas y redes	L1	L2
[OP2.1.1] Existen planes de seguridad documentados para la salvaguarda de sistemas y redes.	L2	L3
[OP2.1.2] Los planes de seguridad se revisan, comprueban y actualizan periódicamente.	L1	L2
[OP2.1.3] Se protege la información sensible mediante su almacenamiento en condiciones de seguridad, como el que proporcionan	L3	L2
las cadenas de custodia definidas	L3	L2
las copias de respaldo almacenadas fuera de las instalaciones	L3	L2
los medios de almacenamiento separables	L3	L2
un proceso de eliminación de la información sensible o de sus medios de almacenamiento	L3	L2
[OP2.1.4] La integridad del software instalado se verifica regularmente.	L3	L4
[OP2.1.5] Todos los sistemas se encuentran actualizados respecto a revisiones, parches, y recomendaciones en documentos de asesoramiento sobre seguridad.	L2	L4
[OP2.1.6] Existe un plan de copias de respaldo de datos que	L2	L3
se actualiza regularmente	L2	L3
se comprueba periódicamente	L2	L3

requiere la realización de copias de respaldo programadas regularmente, tanto del software, como de los datos	L2	L3
requiere la comprobación y verificación periódicas de la capacidad para restaurar a partir de copias de respaldo	L2	L3
[OP2.1.7] Todo el personal comprende y es capaz de desempeñar sus responsabilidades con arreglo a los planes de respaldo.	L2	L4
[OP2.1.8] Los cambios del hardware y el software de las TI se planifican, supervisan y documentan.	L1	L4
[OP2.1.9] Los miembros del personal de TI siguen los procedimientos pertinentes al publicar, modificar y anular contraseñas, cuentas y privilegios de usuario.	L2	L2
Se requiere una identificación única de usuario para todos los usuarios del sistema de información, incluidos los usuarios terceros.	L2	L2
Las cuentas y contraseñas por defecto han sido suprimidas de los sistemas.	L2	L2
[OP2.1.10] Sólo operan en los sistemas los servicios necesarios; todos los innecesarios se han suprimido.	L1	L4
[OP2.2] Herramientas de administración de sistemas	L1	L2
[OP2.2.1] Los nuevos instrumentos de seguridad, procedimientos y mecanismos se revisan de manera ordinaria para determinar su aplicabilidad en la consecución de las estrategias de seguridad de la organización.	L2	L2
[OP2.2.2] Las herramientas y los mecanismos para conseguir el uso de una administración de sistemas y de red segura, y su revisión y actualización o sustitución con carácter periódico. Son ejemplos de estas herramientas los que siguen:	L1	L2
comprobadores de la integridad de los datos	L1	L2
herramientas de codificación	L1	L2
escáneres de vulnerabilidades	L1	L2
herramientas de comprobación de la calidad de las contraseñas	L1	L2
escáneres de virus	L3	L2
herramientas de gestión de procesos	L1	L2
sistemas de detección de intrusos	L1	L2
administraciones remotas seguras	L2	L2
herramientas de servicio de red	L1	L2
analizadores de tráfico	L1	L2
herramientas de respuesta en caso de incidente	L1	L2
herramientas forenses para el análisis de datos	L1	L2
[OP2.3] Seguimiento y auditoría de la seguridad física	L1	L2
[OP2.3.1] La organización utiliza de manera ordinaria herramientas de seguimiento y auditoría de sistemas y redes.	L1	L2
La actividad es objeto de seguimiento por parte del personal de TI.	L1	L2
Se registra la actividad de sistemas y redes.	L2	L2
Los registros se revisan regularmente.	L1	L2
La actividad inusual se trata con arreglo a la política o el procedimiento pertinentes.	L1	L2
Las herramientas se revisan y actualizan periódicamente.	L1	L2
[OP2.3.2] Los cortafuegos y otros componentes de seguridad se auditan periódicamente para determinar su conformidad con la política pertinente.	L1	L2
[OP2.4] Autenticación y autorización	L1	L3
[OP2.4.1] Se utilizan controles de acceso y mecanismos de autenticación de usuario apropiados (p. Ej., permisos de archivo,	L2	L3

configuración de red) coherentes con la política establecida al respecto, con el fin de restringir el acceso de los usuarios a		
la información	L2	L3
las utilidades del sistema	L2	L3
el código fuente de programas	L2	L3
los sistemas sensibles	L2	L3
determinadas aplicaciones y servicios	L2	L3
conexiones de red en la organización	L2	L3
conexiones de red con origen fuera de la organización	L2	L3
[OP2.4.2] Existen políticas y procedimientos de uso de la información documentados respecto al acceso individual y en grupo con el fin de:	L2	L3
establecer las normas de concesión del nivel pertinente de acceso	L2	L3
establecer un derecho inicial de acceso	L2	L3
modificar el derecho de acceso	L2	L3
anular el derecho de acceso	L2	L3
revisar y comprobar periódicamente los derechos de acceso	L2	L3
[OP2.4.3] Los métodos y mecanismos de control de acceso restringen el acceso a los recursos con arreglo a los derechos determinados en políticas y procedimientos.	L2	L4
[OP2.4.4] Los métodos y mecanismos de control de acceso se revisan y comprueban periódicamente.	L1	L4
[OP2.4.5] Se dotan métodos o mecanismos para garantizar que la información sensible no es objeto de acceso, alteración o destrucción de un modo no autorizado.	L2	L3
[OP2.4.6] Se utilizan mecanismos de autenticación para proteger la disponibilidad, integridad y confidencialidad de la información sensible. Son ejemplos de estos instrumentos los que siguen:	L2	L3
las firmas digitales	L2	L3
la biometría	L2	L3
[OP2.5] Gestión de vulnerabilidades	L1	L2
[OP2.5.1] Existe un conjunto documentado de procedimientos para la gestión de vulnerabilidades, entre los que figuran:	L1	L2
la selección de herramientas de evaluación de vulnerabilidades, listas de comprobación y scripts	L1	L2
el mantenimiento al día respecto a los tipos de vulnerabilidades conocidos y los métodos de ataque	L1	L2
la revisión de fuentes de información sobre anuncios de vulnerabilidad, alertas de seguridad y notificaciones	L1	L2
la identificación de componentes de infraestructura para su evaluación	L1	L2
la programación de evaluaciones de vulnerabilidad	L1	L2
la interpretación de resultados y la respuesta a éstos	L1	L2
el mantenimiento de un almacenamiento seguro y la disposición de datos sobre vulnerabilidad	L1	L2
[OP2.5.2] Los procedimientos de gestión de vulnerabilidades son objeto de seguimiento, así como de revisiones y actualizaciones periódicas.	L1	L2
[OP2.5.3] Las evaluaciones de vulnerabilidad de la tecnología se realizan de manera periódica, y las vulnerabilidades se tratan cuando se detectan.	L1	L4
[OP2.6] Codificación	L0	L3
[OP2.6.1] Se utilizan controles de seguridad apropiados para proteger la información sensible durante su almacenamiento o transmisión,	L0	L3

incluidos		
el cifrado de datos durante la transmisión	L0	L3
el cifrado de datos al escribir en disco	L0	L3
el uso de infraestructura de claves públicas	L0	L3
la tecnología de redes privadas virtuales	L0	L3
el cifrado de todas las transmisiones a través de Internet	L1	L3
[OP2.6.2] Se utilizan protocolos cifrados cuando se gestionan de manera remota sistemas, enrutadores y cortafuegos	L2	L3
[OP2.6.3] Los controles y protocolos de cifrado se someten a revisiones y comprobaciones periódicas	L1	L3
[OP2.7] Diseño y arquitectura de seguridad	L0	L2
[OP2.7.1] En la arquitectura y el diseño de sistemas nuevos y revisados se tienen en cuenta	L2	L2
las estrategias, políticas y procedimientos de seguridad	L2	L2
el historial de situaciones de riesgo en materia de seguridad	L2	L2
los resultados de las evaluaciones de riesgos para la seguridad	L2	L2
[OP2.7.2] La organización dispone de diagramas actualizados que muestren la tipología de red y la arquitectura de seguridad del conjunto de la empresa.	L0	L4

Comentarios

[OP3] Seguridad del personal

salvaguarda	[presente]	[objetivo]
[OP3.1] Gestión de incidentes	L0	L3
[OP3.1.1] Existen procedimientos documentados para la identificación de presuntos incidentes e infracciones de seguridad, así como para la elaboración de informes al respecto, y para la adopción de respuestas a los mismos, entre los que figuran:	L1	L3
los incidentes que atañen a las redes	L1	L3
los incidentes relativos al acceso físico	L1	L3
los incidentes de ingeniería social	L1	L3
[OP3.1.2] Los procedimientos de gestión de incidentes se comprueban, verifican y actualizan periódicamente.	L0	L3
[OP3.1.3] Existen políticas y procedimientos documentados respecto a la colaboración con los órganos encargados de velar por el cumplimiento de las leyes.	L2	L3
[OP3.2] Prácticas de personal generales	L1	L2
[OP3.2.1]Los miembros del personal se atienen a buenas prácticas en materia de seguridad, como las que siguen:	L1	L2
asegurar la información respecto a la que son responsables	L2	L2
abstenerse de divulgar información sensible a terceros (resistencia a la ingeniería social)	L1	L2
disponer de la capacidad adecuada para utilizar los equipos y el software de las tecnologías de la información	L2	L2
utilizar buenas prácticas en lo que se refiere a las contraseñas	L1	L2
comprender y observar las políticas y reglamentos de seguridad	L1	L2
reconocer los incidentes e informar de éstos	L1	L2
[OP3.2.2] Todo el personal, a todas las escalas de responsabilidad, desempeña las funciones que se le han asignado y asume sus responsabilidades en lo que atañe a la seguridad de la información.	L2	L3
[OP3.2.3] Existen procedimientos documentados para autorizar y supervisar a aquéllos que manejan información sensible o trabajan en	L1	L2

emplazamientos en los que se deposita la misma. Se trata de:		
empleados	L2	L2
contratistas, socios, colaboradores, y personal de entidades terceras	L1	L2
personal de mantenimiento de sistemas	L1	L2
personal de mantenimiento de instalaciones	L1	L2

Comentarios

Informe de Análisis de Riesgos 30.9.2008

(SME C)

Preparado:	GMV Soluciones Globales Internet		Clasification Type After Sanitization: UNCLASSIFIED
Verificado:	N/A	Código:	SGI-ERNSTING-INF-XXX
Aprobado:	Mª Teresa Avelino Carmona	Versión:	1
Autorizado:	Mª Teresa Avelino Carmona	Fecha:	30/09/2008

GMV SOLUCIONES GLOBALES INTERNET S.A.
P.T. Boecillo Parcela 101 - 47151 Valladolid.
Tel.: +34 983 54 65 54, Fax: +34 983 54 65 53.
www.gmv-sgi.es, www.gmv.com.

Código Interno: SGISA xxx/08

ESTA PÁGINA SE HA DEJADO EN BLANCO INTENCIONADAMENTE.

HOJA DE ESTADO DEL DOCUMENTO

Versión	Fecha	Págs.	Procesador	Cambios
1	30/09/2008	37	Word 2000 español	Primera versión

ÍNDICE

LISTA DE TABLAS Y FIGURAS

1. INTRODUCCIÓN

1.1. PROPÓSITO

El objeto del presente documento es plasmar los resultados obtenidos tras el análisis de riesgos realizado sobre los activos de información e instalaciones englobados en el alcance del mismo. Este análisis de riesgos se ha realizado dentro del ámbito de desarrollo del piloto de ENISA para la aplicación de su metodología adaptada a PYMES de análisis de riesgos, haciendo uso de la herramienta Pilar Basic 4.3 como apoyo para la aplicación de dicha metodología.

1.2. ALCANCE

El alcance del presente documento abarca las instalaciones y activos de información relativos a la actividad desarrollada en la sede de empresa C ubicada en X[1]

1.3. DEFINICIONES Y ACRÓNIMOS

1.3.1. DEFINICIONES

Concepto	Definición
Activo	Elementos del sistema de información que aportan valor a la organización
Confidencialidad	Garantía de que la información es accesible sólo a aquellas personas autorizadas a tener acceso a ella.
Disponibilidad	Garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.
Integridad	Garantía de que se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
Autenticación	Identificación de quién hace uso de los datos o servicios
Amenaza	Sucesos que pueden materializarse causando un perjuicio a la organización
Vulnerabilidad	Posibilidad de materialización de una amenaza sobre un activo
Riesgo	Índice que integra la probabilidad de que un escenario se materialice y la degradación que supondría sobre un activo
Impacto	Índice de daño o presión al que se ve sometido un servicio, proceso o activo en caso de la materialización de una amenaza
Salvaguardas	Elementos de defensa desplegados para reducir el perjuicio para la organización en caso de materialización de una amenaza

1.3.2. ACRÓNIMOS

Acrónimo	Concepto
[D]	Disponibilidad
[I]	Integridad
[C]	Confidencialidad
UE	Unión Europea

[1] SME name and location

2. REFERENCIAS

Los siguientes documentos son aplicables en la medida que tengan carácter contractual o hayan sido aprobados por el cliente, correspondiéndose sus versiones y fechas con las vigentes en el momento de publicación del presente documento; el resto se han usado simplemente a modo de soporte.

Código	Documento
[ENISA-INF]	Paquete informativo para PYME
[MAGERITV2]	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

3. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS[2]

Hoy en día nos encontramos en un entorno en el que la información se ha convertido en uno de los principales activos de cualquier organización. Se debe entender información en un sentido amplio, independientemente de la forma en la que se guarde o se transmita. Por lo tanto, esta información debe gestionarse y protegerse estratégicamente y de forma proactiva, incluyendo los sistemas y equipos o recursos que contribuyen a su almacenamiento, proceso y transmisión.

La gestión y protección de la información crítica de la organización deber realizarse de forma inteligente, identificando los procesos de negocio, los componentes que sustentan dichos procesos y las amenazas potenciales que podrían poner en peligro la normal ejecución de los mismos. Este esfuerzo de identificación y análisis debe facilitar la toma de decisiones en cuestión de seguridad, permitiendo priorizar las actuaciones que deben realizarse y optimizar el uso de los recursos. Esta tarea de análisis para la identificación de los puntos críticos de negocio y de las principales amenazas es una práctica que debe aplicarse de forma global y sistemática en el transcurso de la actividad diaria de la organización con el fin de invertir en seguridad de una forma racional, protegiendo aquellos activos que lo necesitan y con la intensidad necesaria.

Es aquí donde entra en juego el análisis de riesgos, que pretende sistematizar todo este proceso de análisis e identificación de actividades críticas para el negocio y amenazas potenciales con el fin de estimar la magnitud de los riesgos a los que está expuesta una organización. Esto permitirá conocer el estado actual de la organización en materia de seguridad, de forma que se pueda realizar una gestión adecuada de los riesgos identificados. Esta gestión de los riesgos consistirá en la planificación e implantación de las salvaguardas adecuadas de acuerdo a los objetivos, política y estrategia de la organización con el fin de reducir, transferir o asumir dichos riesgos. El riesgo no se puede erradicará totalmente, sino que el objetivo será reducirle a un nivel residual que sea asumible para la organización.

De forma general se puede dividir el proceso de análisis de riesgos en cuatro fases diferenciadas:

1. Identificación de activos relevantes para la organización. Entendiendo activo como cualquier recurso de información o relacionado con ésta necesario para la correcta ejecución de la actividad de la organización. Es obvio que no todos los activos son iguales, sino que pertenecerán a diferentes categorías (red, hardware, software, personas, etc.), lo cual condicionará las potenciales amenazas y las salvaguardas aplicables.
2. Identificación de amenazas. Amenazas son todos aquellos sucesos que pueden ocurrir y que puede causar un perjuicio a la organización. No todas las amenazas afectan a todos los activos, sino que hay una dependencia directa entre el tipo de activo y lo que le podría ocurrir. Así, podrían extorsionar a un empleado de la organización, mientras que no ocurre lo mismo con una aplicación o un servidor. De igual forma, no todos los activos se ven afectados de igual manera ni en el mismo grado por una determinada amenaza, por lo tanto es importante estimar cómo de vulnerable es un determinado activo atendiendo a dos aspectos:
    - Degradación: Cómo de perjudicado se vería el activo ante la materialización de la amenaza. Suele expresarse como un porcentaje del valor del activo.
    - Frecuencia: Cada cuanto es probable que se materialice la amenaza. Proporciona una nueva dimensión a la degradación que puede causar una amenaza, ya que una amenaza puede ser de terribles consecuencias pero de muy probable

[2] Here comes a short description about risk analysis process for an easier understanding of the report and the concepts used on it. a short explanation about the ENISA approach is also included in this section

materialización otra podría ser de muy bajas consecuencias pero tan frecuente como para acabar acumulando un daño considerable.

Mientras que estos dos aspectos nos determinan la forma en que una amenaza puede afectar un activo, es necesario determinar en qué sentido se puede producir este perjuicio. Para ello se pueden considerar tres dimensiones en las que un activo de información podría verse afectado:

- Disponibilidad: Se debe evaluar el perjuicio de que el activo no esté o no pueda ser utilizado.
- Confidencialidad: Se debe evaluar el perjuicio de que la información sea conocida por quien no debe.
- Integridad: Se debe valorar el perjuicio de que el activo o la información pueda estar manipulada, dañada o corrupta.

3. Identificación de salvaguardas existentes. Hasta este punto no se han tenido en cuenta las salvaguardas desplegadas, se tiene por lo tanto un mapa del riesgo potencial de la organización en el que se determinan los impactos y riesgos a que estarían expuestos los activos si no se protegieran, lo cual no es habitual. Las salvaguardas pueden tener dos efectos en el riesgo presente, bien reduciendo la frecuencia o la probabilidad de que una amenaza se materialice (salvaguardas preventivas) o bien limitando el impacto producido por una amenaza. Se puede considerar una salvaguarda efectiva al 100% cuando:

   - Es teóricamente idónea
   - Está perfectamente desplegada, configurada y mantenida
   - Se emplea siempre
   - Existen procedimientos claros de uso normal y en caso de incidencias
   - Los usuarios están formados y concienciados
   - Existen controles que avisan de posibles fallos

La forma en que se relacionan todos estos elementos se muestra en la siguiente figura:

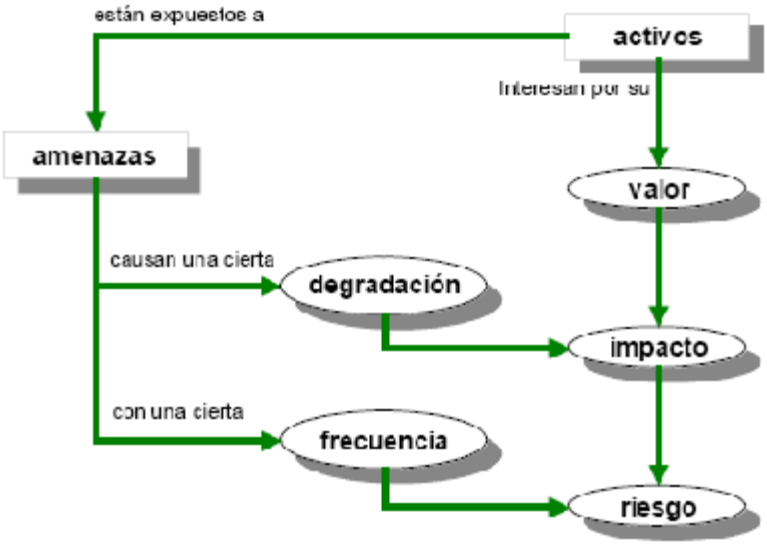

Figura 1: Relación de conceptos en el mapa de riesgos potencial

Una vez finalizado el análisis de riesgos se debe haber obtenido una visión de los impactos y riesgos residuales de la organización con las salvaguardas existentes. En el caso de que el riesgo residual no sea despreciable o asumible por la organización se tendrán que planificar y adoptar medidas que permitan alcanzar ese nivel de riesgo asumible para la organización. Es esto lo que se entiende por Gestión del Riesgo.

Durante el proceso de gestión del riesgo se deben seleccionar de forma prioritaria aquellas salvaguardas de tipo preventivo que permitan minimizar la probabilidad de que las amenazas se materialicen o que el daño producido sea despreciable. No obstante, dado que esto no es siempre posible, se deben adoptar en cualquier caso las medidas necesarias para que un posible incidente de seguridad no pase inadvertido, permitiendo su pronta detección, una reacción adecuada mediante un plan de emergencia y la posibilidad de recuperar el sistema a sus condiciones aceptables de funcionamiento lo antes posible mediante la elaboración de planes de continuidad.

Por último, debe tenerse en cuenta que una aplicación de salvaguardas eficiente debe llegar a un cierto equilibrio entre:

- Salvaguardas técnicas: en aplicaciones, equipos y comunicaciones
- Salvaguardas físicas: protegiendo el entorno de trabajo de las personas y los equipos
- Medidas de organización: de prevención y gestión de las incidencias
- Política de personal: siendo el factor humano el eslabón más débil de la seguridad, resulta de vital importancia contar con medidas adecuadas de contratación de personal, formación continua en buenas prácticas de seguridad, fomentar la participación en el reporte de incidencias y la aplicación de medidas disciplinarias cuando las normativas y política se seguridad de la organización se ven quebrantadas.

En cualquier caso se debe tener siempre presente que el punto óptimo vendrá dado por el equilibrio entre el valor del activo a proteger y la inversión realizada en salvaguardas para

protegerlo, considerando el valor del activo no sólo por su valor económico sino también en términos estratégicos, de reputación, etc.

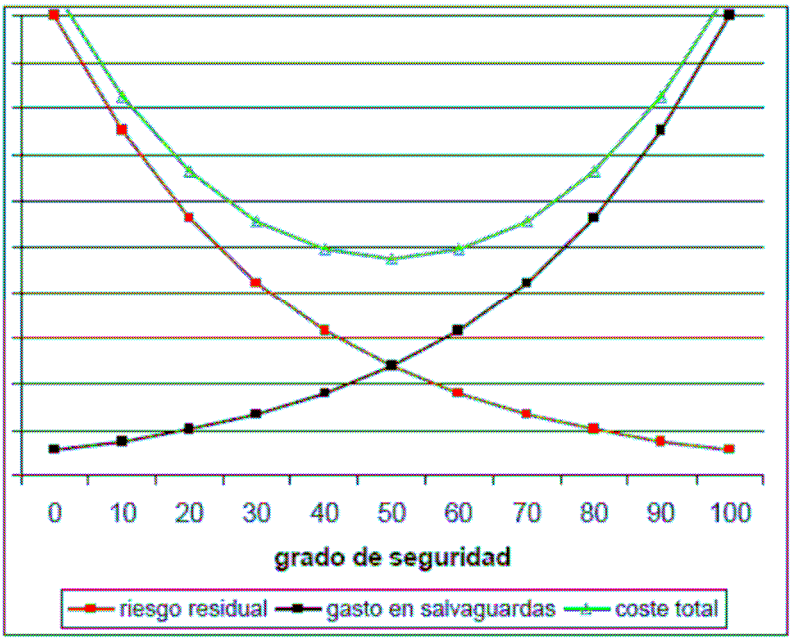

Figura 2: Grado de seguridad

En cuanto al proceso general de análisis de riesgos cabe destacar que existen diferentes metodologías que aportan diferentes enfoques a cada una de las diferentes fases que se pueden diferenciar, no obstante la mayor parte de ellas coinciden en la base conceptual y los objetivos, que han intentado plasmarse en el presente apartado.

El análisis de riesgos realizado dentro del ámbito de este piloto y cuyos resultados se expondrán en el presente documento se basa en la metodología desarrollada por ENISA. El principal objetivo de dicha metodología es la elaboración de un modelo simplificado de análisis de riesgos enfocado a pequeñas organizaciones que permita a dichas organizaciones realizar una evaluación del riesgo presente en sus entornos y seleccionar las medidas pertinentes para gestionar los riesgos identificados con un esfuerzo proporcional a sus recursos.

La metodología ENISA se basa en un enfoque en cuatro fases que tratan los siguientes aspectos:

1. Selección del perfil de riesgos: En esta fase se evalúa el perfil de riesgo de la organización mediante la utilización de un conjunto predefinido de criterios estructurados en una tabla de evaluación en la que la organización debe situarse.
2. Identificación de los activos críticos: En esta fase se seleccionan los activos más importantes en los procesos de negocio de la organización definiendo los requisitos de seguridad para cada uno de dichos activos y clasificándoles según su naturaleza.
3. Selección de tarjetas de controles o salvaguardas: Basándose en el perfil de riesgo de la organización y los requisitos de seguridad definidos para los activos de la empresa se seleccionan unos controles o salvaguardas aplicables.
4. Ejecución y gestión: Una vez determinados todos los aspectos anteriores y analizada la situación actual frente a la deseada se deben asignar prioridades en la ejecución de los controles.

Como herramienta de apoyo para aplicar la metodología se ha hecho uso de la aplicación Pilar Basic 4.3, resultado de la adaptación a la metodología ENISA de la herramienta EAR Pilar, ideada como herramienta de ayuda en la realización de los cálculos asociados al análisis de riesgos en sistemas complejos.

4. PERFIL DE RIESGO

La definición del perfil de riesgo según la metodología ENISA se realiza en base a la definición de la situación de la organización de acuerdo a las siguientes áreas y niveles:

Áreas de riesgo	Alto	Medio	Bajo
Riesgos jurídicos	La empresa maneja información de los clientes de carácter sensible y personal, incluidas historias médicas y datos personales críticos, con arreglo a lo previsto en la legislación de protección de datos de la UE	La empresa maneja la información de los clientes de índole personal, pero no sensible, conforme se define ésta en la Ley de protección de datos de la UE	La empresa no maneja datos personales distintos a los del personal empleado por ella
Riesgos de productividad	La empresa emplea a más de 100 personas que requieren a diario del acceso a aplicaciones y servicios empresariales	La empresa emplea a más de 50 personas que requieren a diario del acceso a aplicaciones y servicios empresariales	La empresa emplea a menos de 10 personas que requieren a diario del acceso a aplicaciones y servicios empresariales
Riesgos para la estabilidad financiera	Los ingresos anuales exceden de 25 millones de euros y/o las transacciones financieras con terceros o clientes tienen lugar como proceso habitual parte de su actividad empresarial	Los ingresos anuales no exceden de 25 millones de euros	Los ingresos anuales no exceden de 5 millones de euros
Riesgos para la reputación y de pérdida de confianza de los clientes	La indisponibilidad o la calidad del servicio repercuten directamente en el perfil empresarial, y/o más del 70% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa	La indisponibilidad o la calidad del servicio pueden repercutir indirectamente en el perfil empresarial, y/o menos del 5% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa	La indisponibilidad o la calidad del servicio no pueden repercutir de manera directa o indirecta en el perfil empresarial, ni derivar en pérdida de ingresos

Tabla 1: Criterios de definición del perfil de riesgos

En el caso que nos ocupa, la empresa C centra su actividad en XXXX[3]

[3] Here there come the comments over the reasons why we chose the risk profile based on the table about and the answers made to questions in the questionnaire and another one regarded with the SME business environment

Por lo tanto de acuerdo a las características de la empresa analizada y en base a los criterios definidos en la metodología ENISA de análisis de riesgos y según la percepción de la propia empresa, se pueden determinar los niveles de riesgo que se muestran en la siguiente tabla, siendo el valor más alto y el que determina el perfil de riesgo global de la empresa "**Medio**"[4]

Áreas de riesgo	Nivel de riesgo	Perfil de Riesgo
Riesgos jurídicos (*Legal and Regulatory*)	Bajo (*Low*)	Medio *(Medium)*
Riesgos de productividad (*Productivity*)	Medio (*Medium*)	
Riesgos para la estabilidad financiera (*Financial Stability*)	Bajo (*Low*)	
Riesgos para la reputación y de pérdida de confianza de los clientes (*Reputation and Loss of Customer Confidence*)	Bajo (*Low*)	

Tabla 2: Perfil de riesgo de la empresa

[4] Risk profile selection for each defined risk area

5. ACTIVOS CRÍTICOS

Tal y como se ha explicado en el apartado anterior, se han identificado dos actividades críticas para la empresa C[5]:

- XXXXXXXX
- XXXXXXXX

De forma adicional se puede destacar que la empresa dispone de portal web y servicio de correo electrónico en régimen de hosting.

Teniendo en cuenta los datos anteriores y la entrevista mantenida con los responsables de la empresa se han identificado y clasificado los siguientes activos críticos que serán incluidos en el análisis de riesgos:[6]

- Aplicaciones (*Applications*):
  - [information repository 1]
  - [information repository 2]
  - [information repository 3]
  - [information repository 4]
- Equipos (*Systems*)
  - [Archiving, NAS, BBDD]
  - [Web Server, Mail Server, firewall]
  - [workstations]
  - [Archiving and Backup]
  - [Important process monitoring]
- Comunicaciones (*Network*)
  - [Cabling, routers and network segments, PABX, wifi]
- Personal (*People*)
  - [Operation and technology1]
  - [Operation and technology2]
  - [Administrative assistants and human resources management]
  - [Contractors and Third Parties]

[5] Critical Business activities identification

[6] Assets identification

De acuerdo a la metodología ENISA los activos enumerados pueden englobarse dentro de las siguientes categorías:[7]

Activo crítico (Critical Asset)	Categoría de activo (*Asset category*)	Componentes (*Components*)	Requisitos de seguridad (*Security requirements*)	Justificación de su selección (*Justification*)
Repositorios de información de I+D (*I+D information repositories*)	Sistemas (*Systems*)	Todos los activos definidos en este apartado	Confidencialidad (Confidentiality) Integridad (Integrity) Disponibilidad (Availability)	XXXXX

Tabla 3: Activos seleccionados

[7] Assets categorization and security requirements identification

6. SELECCIÓN DE CONTROLES

La metodología ENISA define una serie de salvaguardas organizativas y orientadas a activos que deben seleccionarse o que son recomendables según el perfil de riesgo de la empresa y los activos críticos de la misma.

Según el perfil de riesgo definido para cada una de las áreas y teniendo en cuenta las especificaciones de la metodología ENISA se pueden seleccionar los siguientes controles:[8]

Áreas de riesgo (*Risk areas*)	Nivel de riesgo (*Risk level*)	Controles organizativos (*Organizational controls*)
Riesgos jurídicos (*Legal and Regulatory*)	Bajo (*Low*)	SP1.1
Riesgos de productividad (*Productivity*)	Medio (*Medium*)	SP4 SP6
Riesgos para la estabilidad financiera (*Financial Stability*)	Bajo (*Low*)	SP4.1
Riesgos para la reputación y de pérdida de confianza de los clientes (*Reputation and Loss of Customer Confidence*)	Bajo (*Low*)	SP4.1

Tabla 4: Salvaguardas organizativas recomendadas

[8] Organizational controls

Basándonos en el perfil de riesgos global y la categorización de los activos, según la metodología ENISA se deben seleccionar los controles pertenecientes al grupo CC-2S que agrupa las siguientes salvaguardas:[9]

Identificación de la tarjeta de controles basados en los activos (*Asset Bases Control card ID*)										
	CC-2S									
Perfil de riesgos (*Risk profile*)										
	Medio									
Categoría del activo (*Asset category*)										
	Sistema									
Requisitos de seguridad (*Security requirements*)	Seguridad Física (*Physical Security*)	Gestión de sistemas y redes (*System and network Management*)	Herramientas de administración de sistemas (*System Administration tools*)	Seguimiento y auditoría de la seguridad física (*Monitoring and Auditing IT Security*)	Autenticación y autorización (*Authenticatioon and Authorization*)	Gestión de vulnerabilidades (*Vulnerability Management*)	Cifrado (*Encryption*)	Diseño y arquitectura de seguridad (*Securioty Architecture and Design*)	Gestión de incidentes (*Incident Management*)	Prácticas de personal generales (*General Staff practices*)
Confidencialidad (*Condifentiality*)		2.1.6 2.1.7			2.4.1					
Integridad (*Integrity*)		2.1.9			2.4.1					
Disponibilidad (*Availability*)		2.1.6 2.1.7								

Tabla 5: Salvaguardas orientada a activos recomendadas

[9] Score card selection and asset based controls

De esta forma se pueden concluir los siguientes controles a implantar en el sistema:

Activo	Control	Justificación de su selección
Controles basados en los activos	OP2.1.6 OP2.1.7 OP2.1.9 OP2.4.1	Los controles de autenticación y autorización, así como la realización de copias y gestión de contraseñas son de gran importancia para mantener la integridad, confidencialidad y disponibilidad del activo objeto en consideración
Controles organizativos	SP1.1	Formación y sensibilización en responsabilidades de seguridad
	SP4	Política de seguridad
	SP6	Planificación de Contingencias / recuperación en caso de catástrofe

Tabla 6: Salvaguardas recomendadas

En los siguientes aparatados del presente documento se profundiza en los aspectos incluidos en cada una de los controles recomendados, así como en el análisis entre el estado actual de implantación y el nivel recomendado de los mismos.

7. ANÁLISIS DEL ESTADO ACTUAL VS OBJETIVO

Con el objetivo de realizar una gestión y priorización adecuada de los controles seleccionados, se debe realizar un análisis que nos permita contrastar el estado actual de aplicación de las diferentes salvaguardas en la organización respecto el estado recomendable de las mismas. Para facilitar la realización de este análisis se ha dividido el grado de implantación de las salvaguardas según los siguientes niveles[10]:

- L0. La salvaguarda no se encuentra implantada en la organización.
- L1. En este nivel de madurez, las salvaguardas existen, pero no se gestionan. El éxito depende de buena suerte. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta.
- L2. En este nivel de madurez, la eficacia de las salvaguardas depende de la buena suerte y de la buena voluntad de las personas. Los éxitos son repetibles, pero no hay plan para los incidentes más allá de la reacción heroica. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.
- L3. Se despliegan y se gestionan las salvaguardas. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular de las protecciones. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece.
- L4. Usando medidas de campo, la dirección puede controlar empíricamente la eficacia y la efectividad de las salvaguardas. En particular, la dirección puede fijar metas cuantitativas de la calidad. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa, mientras que en el nivel L3, la confianza era solamente cualitativa.
- L5. Este nivel de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora de los procesos. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.

De esta forma, en las siguientes tablas se plasma para cada una de los grupos de salvaguarda la comparativa entre el estado actual y el estado objetivo o recomendable según el modelado de la metodología ENISA realizado mediante la herramienta Pilar. Las valoraciones asignadas a cada una de las salvaguardas tanto para el estado actual como el objetivo son fruto de la entrevista mantenida con la empresa y la experiencia de la empresa GMV en la realización de análisis de riesgos.

[10] Here comes by safeguard, the tables with the current situation and the regarded situation as ENISA suggests. we have done a gap analysis considering the current situation based on the meeting held with the SME. the maturity level for each control has been evaluated in six levels l0-l5 in order to simplify the gap analysis.

For each table with the safeguards and the evaluation, we have made comments with the justification or any finding that echoes the evidence if required.

[SP1] Formación y sensibilización en materia de seguridad

salvaguarda	[presente]	[objetivo]
[SP1.1] Los miembros del personal comprenden sus funciones y responsabilidades en materia de seguridad. Este hecho está documentado y comprobado.	L2	L4

Comentarios:[11]

[SP4] Políticas y normativas de seguridad

salvaguarda	[presente]	[actual]
[SP4.1] La organización dispone de un conjunto exhaustivo de políticas vigentes y documentadas que se revisan y actualizan periódicamente. Estas políticas abordan áreas temáticas fundamentales en materia de seguridad, entre las que se cuentan:	L1	L2
la gestión y la estrategia de seguridad	L2	L2
la gestión de riesgos para la seguridad	L2	L2
la seguridad física	L1	L2
la gestión de sistemas y redes	L1	L2
las herramientas de administración de sistemas	L1	L2
el seguimiento y la auditoría	L1	L2
la autenticación y la autorización	L1	L2
la gestión de vulnerabilidades	L1	L2
la codificación	L2	L2
la arquitectura y el diseño de la seguridad	L1	L2
la gestión de incidentes	L1	L2
las prácticas de seguridad de personal	L2	L2
la legislación aplicable	L1	L2
la sensibilización y la formación	L1	L2
la seguridad de la información basada en la colaboración	L1	L2
la planificación de contingencias y la recuperación en caso de catástrofe	L1	L2
[SP4.2] Existe un proceso documentado para la gestión de políticas de seguridad, incluidas las tareas de:	L2	L2
creación	L2	L2
administración (incluidas revisiones y actualizaciones periódicas)	L2	L2
comunicación	L2	L2
[SP4.3] La organización cuenta con un proceso documentado para la evaluación periódica (técnica y no técnica) del cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L2	L3

[11] Regarded comments. Example: Staff members apply common security practices based on their own knowledge. These practices are not documented or linked with internal policy or employee's contracts.

Organization common security practices should be documented and included in the internal training program. In addition, staff members should sign non disclosure agreements at the beginning of working relationship. …

[SP4.4] La organización cuenta con un proceso documentado para garantizar el cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L1	L3
[SP4.5] La organización aplica de manera uniforme sus políticas de seguridad.	L2	L3
[SP4.6] Únicamente el personal autorizado puede comprobar y revisar las políticas y procedimientos de seguridad.	L2	L3

Comentarios:

[SP6] Planificación de contingencias / recuperación en caso de catástrofe

salvaguarda	[presente]	[objetivo]
[SP6.1] Se ha efectuado un análisis de operaciones, aplicaciones y de la significación de los datos.	L2	L3
[SP6.2] La organización ha documentado	L1	L3
los planes de continuidad de la actividad empresarial y de operación en casos de emergencia	L1	L3
los planes de recuperación en caso de catástrofe	L1	L3
los planes de contingencia para la respuesta en casos de emergencia	L1	L3
[SP6.3] En los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial se consideran los requisitos y conrtroles de acceso físico y electrónico.	L1	L2
[SP6.4] Los planes de contingencia, recuperación en caso de catástrofe, y continuidad de la actividad empresarial se revisan y comprueban periódicamente.	L1	L2
[SP6.5] Todo el personal ...	L1	L3
tiene conocimiento de los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial	L1	L3
comprende sus responsabilidades y está capacitado para cumplirlas	L1	L3

Comentarios

[OP2] Seguridad de las tecnologías de la información

salvaguarda	[presente]	[objetivo]
[OP2.1.6] Existe un plan de copias de respaldo de datos que	L2	L3
se actualiza regularmente	L2	L3
se comprueba periódicamente	L2	L3
requiere la realización de copias de respaldo programadas regularmente, tanto del software, como de los datos	L2	L3
requiere la comprobación y verificación periódicas de la capacidad para restaurar a partir de copias de respaldo	L2	L3
[OP2.1.7] Todo el personal comprende y es capaz de desempeñar sus responsabilidades con arreglo a los planes de respaldo.	L1	L3
[OP2.1.9] Los miembros del personal de TI siguen los procedimientos pertinentes al publicar, modificar y anular contraseñas, cuentas y privilegios de usuario.	L1	L3
Se requiere una identificación única de usuario para todos los usuarios del sistema de información, incluidos los usuarios terceros.	L1	L3
Las cuentas y contraseñas por defecto han sido suprimidas de los sistemas.	L1	L3
[OP2.4.1] Se utilizan controles de acceso y mecanismos de autenticación de usuario apropiados (p. ej., permisos de archivo, configuración de red) coherentes con la política establecida al respecto, con el fin de restringir el acceso de los usuarios a	L0	L3

la información	L2	L3
las utilidades del sistema	L0	L3
el código fuente de programas	n.a.	n.a.
los sistemas sensibles	L2	L3
determinadas aplicaciones y servicios	L2	L3
conexiones de red en la organización	L1	L3
conexiones de red con origen fuera de la organización	L0	L3

Comentarios

8. RESUMEN EJECUTIVO

XXXXX[12]

[12] Here comes the most important aspects and recommendations that the SME should take into account with regard to ENISA risk analisys approach and GMV expertise. it includes recommendations about the selected scorecards in ENISA methodology and other relevants aspects

9. ANEXO A: RESULTADOS DE LA HERRAMIENTA PILAR

La herramienta Pilar permite completar los resultados de la metodología ENISA con consideraciones más específicas de análisis de riesgos, enriqueciendo los resultados obtenidos con datos más específicos y gráficos que permiten contrastar de forma rápida y sencilla la evolución del riesgo en la organización respecto al grado de implantación de las salvaguardas.

En cuanto a la selección de amenazas, la herramienta Pilar permite definir las amenazas de interés para cada uno de los activos. Cada una de estas amenazas tendrá asociados unos parámetros de impacto para cada una de las dimensiones de seguridad en caso de materialización y frecuencia de ocurrencia. En la versión utilizada de la herramienta para el desarrollo del piloto, se seleccionan unas amenazas por defecto para cada tipo de activo según su naturaleza, personas, red, hardware, ..., con valores también por defecto para la frecuencia y el impacto. Esto permite al usuario abstraerse de la complejidad asociada a la selección de este tipo de parámetros durante el análisis de riesgos a la vez que se permite desglosar la información del mapa de riesgo por cada una de las amenazas asociadas a los activos. De forma complementaria a las amenazas seleccionadas por defecto la herramienta permite seleccionar amenazas adicionales que permitan adaptarse a los diferentes requisitos del sector de actividad de cada empresa. Las amenazas por defecto para cada uno de los activos que han sido seleccionadas en la herramienta son las siguientes:

Aplicaciones
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.19] Escapes de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.14] Interceptación de información (escucha)
[A.22] Manipulación de programas

Tabla 7: Amenazas de aplicaciones

Equipos
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico

[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.19] Escapes de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.14] Interceptación de información (escucha)
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo

Tabla 8: Amenazas de equipos

Comunicaciones
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia

[E.19] Escapes de información
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.14] Interceptación de información (escucha)
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo

Tabla 9: Amenazas de comunicaciones

Personas
[E.7] Deficiencias en la organización
[E.19] Escapes de información
[E.28] Indisponibilidad del personal
[A.19] Divulgación de información
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)

Tabla 10: Amenazas de personas

En cuanto al mapa de riesgos, la herramienta permite representar de forma gráfica el riesgo presente en la organización en diferentes momentos en función del estado de implantación de las salvaguardas en dichos momentos. En el desarrollo del piloto se han analizado las siguientes estados:[13]

- Riesgo potencial: Riesgo en caso de no existir implantada ninguna salvaguarda.
- Riesgo presente: Riesgo existente en la organización con el estado de implantación actual de las salvaguardas.
- Riesgo objetivo: Riesgo existente en la organización si se implantasen las salvaguardas recomendadas por la metodología ENISA y aquellas recomendaciones fruto de la experiencia de la empresa GMV y los aspectos analizados durante las entrevistas mantenidas con la empresa.

Cada uno de estos mapas de riesgo pueden observarse en las siguientes figuras.

[13] Here comes the potential risk, current risk and target risk images obtained from pilar tool for each SME.

activo	[D]	[I]	[C]
ACTIVOS	{6.3}	{6.3}	{6.3}
[SW] Aplicaciones	{6.3}	{6.3}	{6.3}
[ ]	{6.3}	{6.3}	{6.3}
[ ]	{6.3}	{6.3}	{6.3}
[ ]	{6.3}	{6.3}	{6.3}
[ ]	{6.3}	{6.3}	{6.3}
[HW] Equipos	{6.3}	{6.3}	{6.3}
[ ]	{6.3}	{5.6}	{5.6}
[ ]	{6.3}	{6.3}	{6.3}
[ ]	{6.3}	{6.3}	{6.3}
[ ]	{6.3}	{5.6}	{5.6}
[ ]	{6.3}	{6.3}	{6.3}
[COM] Comunicaciones	{5.9}	{3.3}	{5.9}
[ ]	{5.9}	{3.3}	{5.9}
[P] Personal	{4.3}	{4.9}	{5.0}
[ ]	{4.3}	{4.9}	{5.0}
[ ]	{4.3}	{4.9}	{5.0}
[ ]	{4.0}	{3.5}	{3.6}
[ ]	{4.3}	{4.9}	{5.0}

Figura 3: Riesgo potencial

activo	[D]	[I]	[C]
ACTIVOS	{4.6}	{4.2}	{4.2}
[SW] Aplicaciones	{4.6}	{4.1}	{4.1}
[ ]	{4.6}	{4.1}	{4.1}
[ ]	{4.6}	{4.1}	{4.1}
[ ]	{4.6}	{4.1}	{4.1}
[ ]	{4.6}	{4.1}	{4.1}
[HW] Equipos	{4.6}	{4.2}	{4.2}
[ ]	{4.6}	{4.0}	{3.7}
[ ]	{4.6}	{4.1}	{4.1}
[ ]	{4.6}	{4.2}	{4.2}
[ ]	{4.6}	{4.0}	{3.7}
[ ]	{4.6}	{4.2}	{4.2}
[COM] Comunicaciones	{4.4}	{1.6}	{4.0}
[ ]	{4.4}	{1.6}	{4.0}
[P] Personal	{2.9}	{3.5}	{3.7}
[ ]	{2.9}	{3.5}	{3.7}
[ ]	{2.9}	{3.5}	{3.7}
[ ]	{2.7}	{2.1}	{2.2}
[ ]	{2.9}	{3.5}	{3.7}

Figura 4: Riesgo Presente

activo	[D]	[I]	[C]
ACTIVOS	{1.5}	{1.4}	{1.4}
[SW] Aplicaciones	{1.5}	{1.4}	{1.4}
[ ]	{1.5}	{1.4}	{1.4}
[ ]	{1.5}	{1.4}	{1.4}
[ ]	{1.5}	{1.4}	{1.4}
[ ]	{1.5}	{1.4}	{1.4}
[HW] Equipos	{1.5}	{1.4}	{1.4}
[ ]	{1.4}	{0.7}	{0.7}
[ ]	{1.5}	{1.4}	{1.4}
[ ]	{1.4}	{1.3}	{1.4}
[ ]	{1.4}	{0.7}	{0.7}
[ ]	{1.4}	{1.3}	{1.4}
[COM] Comunicaciones	{1.1}	{0.0}	{1.1}
[ ]	{1.1}	{0.0}	{1.1}
[P] Personal	{0.0}	{0.4}	{0.5}
[ ]	{0.0}	{0.4}	{0.5}
[ ]	{0.0}	{0.4}	{0.5}
[ ]	{0.0}	{0.0}	{0.0}
[ ]	{0.0}	{0.4}	{0.5}

Figura 5: Riesgo objetivo

En el proyecto de la herramienta Pilar proporcionado a la empresa se pueden desglosar cada uno de los mapas de riesgo anteriores en función de las distintas amenazas.

Adicionalmente, el análisis completo de implantación de salvaguardas que se ha tenido en cuenta para la obtención de los mapas de riesgo anteriores se presenta en el Anexo B del presente documento.

10. ANEXO B: ESTADO DE IMPLANTACIÓN DE SALVAGUARDAS[14]

[SP1] Formación y sensibilización en materia de seguridad

salvaguarda	[presente]	[objetivo]
[SP1.1] Los miembros del personal comprenden sus funciones y responsabilidades en materia de seguridad. Este hecho está documentado y comprobado.	L2	L4
[SP1.2] Se dispone de conocimientos técnicos internos adecuados para la totalidad de servicios, mecanismos y tecnologías empleados (p. ej., registro, seguimiento o codificación), incluido el funcionamiento de éstos en condiciones de seguridad. Este hecho está documentado y comprobado.	L2	L2
[SP1.3] Se imparten a todo el personal conocimientos y formación y se le envían recordatorios periódicos en materia de seguridad. El conocimiento del personal está documentado, y la conformidad se comprueba periódicamente. La formación comprende los temas que siguen:	L1	L2
estrategias, metas y objetivos en materia de seguridad	L2	L2
reglamentos, políticas y procedimientos de seguridad	L2	L2
políticas y procedimientos de colaboración con terceros	L1	L2
planes para contingencias y recuperación en caso de catástrofe	L1	L2
requisitos relativos a la seguridad física	L1	L2
perspectiva de los usuarios respecto a	L1	L2
la gestión de sistemas y redes	L1	L2
las herramientas de administración del sistema	L1	L2
el seguimiento y la auditoría en lo que atañe a la seguridad física y asociada a las tecnologías de la información	L1	L2
autenticación y autorización	L1	L2
gestión de vulnerabilidades	L1	L2
codificación	L1	L2
arquitectura y diseño	L1	L2
gestión de incidentes	L1	L2
prácticas generales de personal	L2	L2
observancia de la legislación, sanciones y actuaciones disciplinarias por infracciones de la seguridad	L2	L2
modo de acceder correctamente a la información sensible y trabajo en las áreas en las que ésta es accesible	L2	L2
políticas y procedimientos de extinción de la relación laboral en lo que atañe a la seguridad	L1	L2

Comentarios

[14] Here comes by safeguard, the tables with the current situation and the target situation. in this section, we have included the gap analisys for safeguards not suggested by ENISA approach but GMV consider that are important controls to take into account by the SME.

[SP2] Estrategia de seguridad

salvaguarda	[presente]	[objetivo]
[SP2.1] Las estrategias empresariales de la organización incorporan de manera rutinaria consideraciones de seguridad.	L1	L2
[SP2.2] En las estrategias y políticas de seguridad se tienen en cuenta las estrategias y objetivos empresariales de la organización.	L2	L2
[SP2.3] Las estrategias, metas y objetivos en materia de seguridad se documentan y se revisan, actualizan y comunican periódicamente a la organización.	L1	L2

Comentarios

[SP3] Gestión de seguridad

salvaguarda	[presente]	[objetivo]
[SP3.1] La dirección asigna fondos y recursos suficientes a las actividades de seguridad de la información.	L2	L2
[SP3.2] Se definen funciones y responsabilidades en materia de seguridad para todo el personal de la organización.	L2	L2
[SP3.3] En las prácticas de la organización en materia de contratación y de extinción de la relación laboral con el personal se tienen en cuenta las cuestiones de seguridad de la información.	L1	L2
[SP3.4] Los niveles requeridos de seguridad de la información y el modo en que se aplican a personas y grupos se documentan y aplican.	L1	L2
[SP3.5] La organización gestiona los riesgos que atañen a la seguridad de la información, con inclusión de:	L1	L2
la evaluación de los riesgos para la seguridad de la información, tanto periódicamente, como en respuesta a cambios significativos en la tecnología, amenazas internas o externas, o los sistemas y operaciones de la organización	L2	L2
la adopción de medidas para mitigar los riesgos hasta alcanzar un nivel aceptable	L1	L2
el mantenimiento de un nivel de riesgos aceptable	L1	L2
la utilización de evaluaciones de riesgos para la seguridad de la información con el fin de facilitar la selección de medidas de seguridad y control rentables, equilibrando los costes de ejecución con las posibles pérdidas	L2	L2
[SP3.6] La dirección recibe informes rutinarios, y actúa basándose en ellos, en los que se resumen los resultados de:	L1	L2
la revisión de los registros de sistema	L1	L2
la revisión de los historiales de auditoría	L1	L2
las evaluaciones de vulnerabilidades tecnológicas	L1	L2
los incidentes de seguridad y las respuestas dadas a los mismos	L1	L3
las evaluaciones de riesgos	L1	L3
las revisiones de la seguridad física	L1	L3
los planes y recomendaciones para la mejora de la seguridad	L1	L2

Comentarios

[SP4] Políticas y normativas de seguridad

salvaguarda	[presente]	[actual]
[SP4.1] La organización dispone de un conjunto exhaustivo de políticas vigentes y documentadas que se revisan y actualizan periódicamente. Estas políticas abordan áreas temáticas fundamentales en materia de seguridad, entre las que se cuentan:	L1	L2
la gestión y la estrategia de seguridad	L2	L2

la gestión de riesgos para la seguridad	L2	L2
la seguridad física	L1	L2
la gestión de sistemas y redes	L1	L2
las herramientas de administración de sistemas	L1	L2
el seguimiento y la auditoría	L1	L2
la autenticación y la autorización	L1	L2
la gestión de vulnerabilidades	L1	L2
la codificación	L2	L2
la arquitectura y el diseño de la seguridad	L1	L2
la gestión de incidentes	L1	L2
las prácticas de seguridad de personal	L2	L2
la legislación aplicable	L1	L2
la sensibilización y la formación	L1	L2
la seguridad de la información basada en la colaboración	L1	L2
la planificación de contingencias y la recuperación en caso de catástrofe	L1	L2
[SP4.2] Existe un proceso documentado para la gestión de políticas de seguridad, incluidas las tareas de:	L2	L2
creación	L2	L2
administración (incluidas revisiones y actualizaciones periódicas)	L2	L2
comunicación	L2	L2
[SP4.3] La organización cuenta con un proceso documentado para la evaluación periódica (técnica y no técnica) del cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L2	L3
[SP4.4] La organización cuenta con un proceso documentado para garantizar el cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L1	L3
[SP4.5] La organización aplica de manera uniforme sus políticas de seguridad.	L2	L3
[SP4.6] Únicamente el personal autorizado puede comprobar y revisar las políticas y procedimientos de seguridad.	L2	L3

Comentarios

[SP5] Gestión de la seguridad en régimen de colaboración

salvaguarda	[presente]	[objetivo]
[SP5.1] La organización ha procedido a la documentación, el seguimiento y la ejecución de procedimientos para la protección de su información cuando colabora con entidades externas (p. ej., terceros, colaboradores, subcontratistas o socios).	L3	L3
[SP5.2] La organización ha comprobado que los servicios, mecanismos y tecnologías de seguridad externalizados satisfacen sus necesidades y requisitos.	L3	L3
[SP5.3] La organización documenta, supervisa y aplica estrategias de protección de la información perteneciente a entidades externas a la que se accede desde componentes de su infraestructura, o que es utilizada por su personal.	L3	L3
[SP5.4] La organización ofrece y verifica actividades de sensibilización y formación sobre las políticas y los procedimientos de seguridad de entidades externas para el personal que interactúa con éstas.	L3	L3
[SP5.5] Existen procedimientos documentados respecto al personal externo cuya relación con la organización ha concluido, en los que se especifican las medidas de seguridad pertinentes para finalizar su	L3	L3

posibilidad de acceso. Estos procedimientos se comunican a la organización externa y se coordinan con ella.		

Comentarios

[SP6] Planificación de contingencias / recuperación en caso de catástrofe

salvaguarda	[presente]	[objetivo]
[SP6.1] Se ha efectuado un análisis de operaciones, aplicaciones y de la significación de los datos.	L2	L3
[SP6.2] La organización ha documentado	L1	L3
los planes de continuidad de la actividad empresarial y de operación en casos de emergencia	L1	L3
los planes de recuperación en caso de catástrofe	L1	L3
los planes de contingencia para la respuesta en casos de emergencia	L1	L3
[SP6.3] En los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial se consideran los requisitos y conrtroles de acceso físico y electrónico.	L1	L2
[SP6.4] Los planes de contingencia, recuperación en caso de catástrofe, y continuidad de la actividad empresarial se revisan y comprueban periódicamente.	L1	L2
[SP6.5] Todo el personal ...	L1	L3
tiene conocimiento de los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial	L1	L3
comprende sus responsabilidades y está capacitado para cumplirlas	L1	L3

Comentarios

[OP1] Seguridad física

salvaguarda	[presente]	[objetivo]
[OP1.1] Planes y procedimientos de seguridad física	L1	L2
[OP1.1.1] Existen planes de seguridad de las instalaciones documentados, concebidos para salvaguardar locales, edificios y cualquier otra área restringida.	L3	L3
[OP1.1.2] Estos planes se revisan, comprueban y actualizan periódicamente.	L2	L2
[OP1.1.3] Los procedimientos y mecanismos de seguridad física se comprueban y revisan periódicamente.	L1	L3
[OP1.1.4] Existen políticas y procedimientos documentados para la gestión de visitantes, que incluyen	L1	L3
el registro en la entrada	L1	L3
el acompañamiento por las instalaciones	L1	L3
los registros de acceso	L1	L3
la recepción y los servicios de hospitalidad	L1	L3
[OP1.1.5] Existen políticas y procedimientos documentados para el control físico del hardware y el software, incluidos	L1	L3
terminales, portátiles, módem, componentes inalámbricos y todos los demás elementos utilizados para acceder a la información	L1	L3
el acceso, el almacenamiento y la recuperación de copias de seguridad de datos	L1	L3
el almacenamiento de información sensible en medios físicos y electrónicos	L1	L3
la supresión de información sensible, o de los medios en los que se	L1	L3

encuentra almacenada		
la reutilización y el reciclaje de papel y medios electrónicos.	L1	L3
[OP1.2] Control de acceso físico	L1	L3
[OP1.2.1] Existen políticas y procedimientos documentados respecto al acceso individual y en grupo, que comprenden:	L1	L3
las normas de concesión del nivel pertinente de acceso físico	L1	L3
las normas para la determinación de los derechos iniciales de acceso	L1	L3
la modificación del derecho de acceso	L1	L3
la anulación del derecho de acceso	L1	L3
la revisión y la comprobación periódicas de los derechos de acceso	L1	L3
[OP1.2.2] Existen políticas, procedimientos y mecanismos documentados para controlar el acceso físico a entidades definidas. Se incluyen aquí:	L1	L3
áreas de trabajo	L1	L3
medios de hardware (ordenadores, dispositivos de comunicación, etc.) y de software	L1	L3
[OP1.2.3] Existen procedimientos documentados para verificar la autorización de acceso antes de autorizar el acceso físico.	L1	L3
[OP1.2.4] Los terminales y otros componentes que permiten el acceso a información sensible se encuentran físicamente protegidos con el fin de evitar accesos no autorizados.	L1	L3
[OP1.3] Seguimiento y auditoría de la seguridad física	L1	L3
[OP1.3.1] Se conservan registros de mantenimiento para documentar las reparaciones y modificaciones de los componentes físicos de las instalaciones.	L1	L3
[OP1.3.2] Pueden justificarse las acciones de una persona o de un grupo respecto a la totalidad de medios controlados físicamente.	L1	L3
[OP1.3.3] Se examinan regularmente registros de auditoría y seguimiento para detectar anomalías, y se emprenden acciones correctivas en caso necesario.	L1	L3

Comentarios

[OP2] Seguridad de las tecnologías de la información

salvaguarda	[presente]	[objetivo]
[OP2.1] Gestión de sistemas y redes	L1	L2
[OP2.1.1] Existen planes de seguridad documentados para la salvaguarda de sistemas y redes.	L1	L3
[OP2.1.2] Los planes de seguridad se revisan, comprueban y actualizan periódicamente.	L1	L3
[OP2.1.3] Se protege la información sensible mediante su almacenamiento en condiciones de seguridad, como el que proporcionan	L1	L2
las cadenas de custodia definidas	L1	L2
las copias de respaldo almacenadas fuera de las instalaciones	L1	L2
los medios de almacenamiento separables	L1	L2
un proceso de eliminación de la información sensible o de sus medios de almacenamiento	L1	L2
[OP2.1.4] La integridad del software instalado se verifica regularmente.	L1	L3
[OP2.1.5] Todos los sistemas se encuentran actualizados respecto a revisiones, parches, y recomendaciones en documentos de asesoramiento sobre seguridad.	L2	L3
[OP2.1.6] Existe un plan de copias de respaldo de datos que	L2	L3

se actualiza regularmente	L2	L3
se comprueba periódicamente	L2	L3
requiere la realización de copias de respaldo programadas regularmente, tanto del software, como de los datos	L2	L3
requiere la comprobación y verificación periódicas de la capacidad para restaurar a partir de copias de respaldo	L2	L3
[OP2.1.7] Todo el personal comprende y es capaz de desempeñar sus responsabilidades con arreglo a los planes de respaldo.	L1	L3
[OP2.1.8] Los cambios del hardware y el software de las TI se planifican, supervisan y documentan.	L2	L3
[OP2.1.9] Los miembros del personal de TI siguen los procedimientos pertinentes al publicar, modificar y anular contraseñas, cuentas y privilegios de usuario.	L1	L3
Se requiere una identificación única de usuario para todos los usuarios del sistema de información, incluidos los usuarios terceros.	L1	L3
Las cuentas y contraseñas por defecto han sido suprimidas de los sistemas.	L1	L3
[OP2.1.10] Sólo operan en los sistemas los servicios necesarios; todos los innecesarios se han suprimido.	L2	L3
[OP2.2] Herramientas de administración de sistemas	L0	L2
[OP2.2.1] Los nuevos instrumentos de seguridad, procedimientos y mecanismos se revisan de manera ordinaria para determinar su aplicabilidad en la consecución de las estrategias de seguridad de la organización.	L1	L2
[OP2.2.2] Las herramientas y los mecanismos para conseguir el uso de una administración de sistemas y de red segura, y su revisión y actualización o sustitución con carácter periódico. Son ejemplos de estas herramientas los que siguen:	L0	L2
comprobadores de la integridad de los datos	L0	L2
herramientas de codificación	L2	L2
escáneres de vulnerabilidades	L1	L2
herramientas de comprobación de la calidad de las contraseñas	L1	L3
escáneres de virus	L2	L3
herramientas de gestión de procesos	L1	L2
sistemas de detección de intrusos	L0	L2
administraciones remotas seguras	L0	L2
herramientas de servicio de red	L1	L2
analizadores de tráfico	L1	L2
herramientas de respuesta en caso de incidente	L0	L3
herramientas forenses para el análisis de datos	L1	L3
[OP2.3] Seguimiento y auditoría de la seguridad física	L0	L2
[OP2.3.1] La organización utiliza de manera ordinaria herramientas de seguimiento y auditoría de sistemas y redes.	L1	L2
La actividad es objeto de seguimiento por parte del personal de TI.	L1	L2
Se registra la actividad de sistemas y redes.	L1	L2
Los registros se revisan regularmente.	L1	L2
La actividad inusual se trata con arreglo a la política o el procedimiento pertinentes.	L1	L2
Las herramientas se revisan y actualizan periódicamente.	L1	L2
[OP2.3.2] Los cortafuegos y otros componentes de seguridad se auditan periódicamente para determinar su conformidad con la política pertinente.	L0	L2
[OP2.4] Autenticación y autorización	L0	L3

[OP2.4.1] Se utilizan controles de acceso y mecanismos de autenticación de usuario apropiados (p. ej., permisos de archivo, configuración de red) coherentes con la política establecida al respecto, con el fin de restringir el acceso de los usuarios a	L0	L3
la información	L2	L3
las utilidades del sistema	L0	L3
el código fuente de programas	n.a.	n.a.
los sistemas sensibles	L2	L3
determinadas aplicaciones y servicios	L2	L3
conexiones de red en la organización	L1	L3
conexiones de red con origen fuera de la organización	L0	L3
[OP2.4.2] Existen políticas y procedimientos de uso de la información documentados respecto al acceso individual y en grupo con el fin de:	L2	L3
establecer las normas de concesión del nivel pertinente de acceso	L2	L3
establecer un derecho inicial de acceso	L2	L3
modificar el derecho de acceso	L2	L3
anular el derecho de acceso	L2	L3
revisar y comprobar periódicamente los derechos de acceso	L2	L3
[OP2.4.3] Los métodos y mecanismos de control de acceso restringen el acceso a los recursos con arreglo a los derechos determinados en políticas y procedimientos.	L2	L4
[OP2.4.4] Los métodos y mecanismos de control de acceso se revisan y comprueban periódicamente.	L1	L4
[OP2.4.5] Se dotan métodos o mecanismos para garantizar que la información sensible no es objeto de acceso, alteración o destrucción de un modo no autorizado.	L1	L3
[OP2.4.6] Se utilizan mecanismos de autenticación para proteger la disponibilidad, integridad y confidencialidad de la información sensible. Son ejemplos de estos instrumentos los que siguen:	L1	L3
las firmas digitales	L1	L3
la biometría	L1	L3
[OP2.5] Gestión de vulnerabilidades	L1	L2
[OP2.5.1] Existe un conjunto documentado de procedimientos para la gestión de vulnerabilidades, entre los que figuran:	L2	L2
la selección de herramientas de evaluación de vulnerabilidades, listas de comprobación y scripts	L2	L2
el mantenimiento al día respecto a los tipos de vulnerabilidades conocidos y los métodos de ataque	L2	L2
la revisión de fuentes de información sobre anuncios de vulnerabilidad, alertas de seguridad y notificaciones	L2	L2
la identificación de componentes de infraestructura para su evaluación	L2	L2
la programación de evaluaciones de vulnerabilidad	L2	L2
la interpretación de resultados y la respuesta a éstos	L2	L2
el mantenimiento de un almacenamiento seguro y la disposición de datos sobre vulnerabilidad	L2	L2
[OP2.5.2] Los procedimientos de gestión de vulnerabilidades son objeto de seguimiento, así como de revisiones y actualizaciones periódicas.	L1	L2
[OP2.5.3] Las evaluaciones de vulnerabilidad de la tecnología se realizan de manera periódica, y las vulnerabilidades se tratan cuando se detectan.	L1	L3
[OP2.6] Codificación	L1	L3

[OP2.6.1] Se utilizan controles de seguridad apropiados para proteger la información sensible durante su almacenamiento o transmisión, incluidos	L3	L3
el cifrado de datos durante la transmisión	L3	L3
el cifrado de datos al escribir en disco	L3	L3
el uso de infraestructura de claves públicas	L3	L3
la tecnología de redes privadas virtuales	L3	L3
el cifrado de todas las transmisiones a través de Internet	L3	L3
[OP2.6.2] Se utilizan protocolos cifrados cuando se gestionan de manera remota sistemas, enrutadores y cortafuegos	L1	L3
[OP2.6.3] Los controles y protocolos de cifrado se someten a revisiones y comprobaciones periódicas	L1	L3
[OP2.7] Diseño y arquitectura de seguridad	L0	L2
[OP2.7.1] En la arquitectura y el diseño de sistemas nuevos y revisados se tienen en cuenta	L0	L2
las estrategias, políticas y procedimientos de seguridad	L0	L2
el historial de situaciones de riesgo en materia de seguridad	L1	L2
los resultados de las evaluaciones de riesgos para la seguridad	L0	L2
[OP2.7.2] La organización dispone de diagramas actualizados que muestren la tipología de red y la arquitectura de seguridad del conjunto de la empresa.	L0	L3

Comentarios

[OP3] Seguridad del personal

salvaguarda	[presente]	[objetivo]
[OP3.1] Gestión de incidentes	L0	L3
[OP3.1.1] Existen procedimientos documentados para la identificación de presuntos incidentes e infracciones de seguridad, así como para la elaboración de informes al respecto, y para la adopción de respuestas a los mismos, entre los que figuran:	L1	L3
los incidentes que atañen a las redes	L1	L3
los incidentes relativos al acceso físico	L1	L3
los incidentes de ingeniería social	L1	L3
[OP3.1.2] Los procedimientos de gestión de incidentes se comprueban, verifican y actualizan periódicamente.	L0	L3
[OP3.1.3] Existen políticas y procedimientos documentados respecto a la colaboración con los órganos encargados de velar por el cumplimiento de las leyes.	L0	L3
[OP3.2] Prácticas de personal generales	L1	L2
[OP3.2.1]Los miembros del personal se atienen a buenas prácticas en materia de seguridad, como las que siguen:	L1	L2
asegurar la información respecto a la que son responsables	L1	L2
abstenerse de divulgar información sensible a terceros (resistencia a la ingeniería social)	L1	L2
disponer de la capacidad adecuada para utilizar los equipos y el software de las tecnologías de la información	L1	L2
utilizar buenas prácticas en lo que se refiere a las contraseñas	L1	L2
comprender y observar las políticas y reglamentos de seguridad	L1	L2
reconocer los incidentes e informar de éstos	L1	L2
[OP3.2.2] Todo el personal, a todas las escalas de responsabilidad, desempeña las funciones que se le han asignado y asume sus responsabilidades en lo que atañe a la seguridad de la información.	L2	L3

[OP3.2.3] Existen procedimientos documentados para autorizar y supervisar a aquéllos que manejan información sensible o trabajan en emplazamientos en los que se deposita la misma. Se trata de:	L1	L2
empleados	L1	L2
contratistas, socios, colaboradores, y personal de entidades terceras	L1	L2
personal de mantenimiento de sistemas	L1	L2
personal de mantenimiento de instalaciones	L1	L2

Comentarios

Informe de Análisis de Riesgos 30.9.2008

(SME D)

Preparado:	GMV Soluciones Globales Internet		Clasification Type After Sanitization: UNCLASSIFIED
Verificado:	N/A	Código:	SGI-ERNSTING-INF-XXX
Aprobado:	Mª Teresa Avelino Carmona	Versión:	1
Autorizado:	Mª Teresa Avelino Carmona	Fecha:	30/09/2008

GMV SOLUCIONES GLOBALES INTERNET S.A.
P.T. Boecillo Parcela 101 - 47151 Valladolid.
Tel.: +34 983 54 65 54, Fax: +34 983 54 65 53.
www.gmv-sgi.es, www.gmv.com.

Código Interno: SGISA xxx/08

ESTA PÁGINA SE HA DEJADO EN BLANCO INTENCIONADAMENTE.

HOJA DE ESTADO DEL DOCUMENTO

Versión	Fecha	Págs.	Procesador	Cambios
1	15/09/2008	37	Word 2000 español	Primera versión

ÍNDICE

LISTA DE TABLAS Y FIGURAS

1. INTRODUCCIÓN

1.1. PROPÓSITO

El objeto del presente documento es plasmar los resultados obtenidos tras el análisis de riesgos realizado sobre los activos de información e instalaciones englobados en el alcance del mismo. Este análisis de riesgos se ha realizado dentro del ámbito de desarrollo del piloto de ENISA para la aplicación de su metodología adaptada a PYMES de análisis de riesgos, haciendo uso de la herramienta Pilar Basic 4.3 como apoyo para la aplicación de dicha metodología.

1.2. ALCANCE

El alcance del presente documento abarca las instalaciones y activos de información relativos a la actividad desarrollada en la sede de empresa D ubicada en X[1]

1.3. DEFINICIONES Y ACRÓNIMOS

1.3.1. DEFINICIONES

Concepto	Definición
Activo	Elementos del sistema de información que aportan valor a la organización
Confidencialidad	Garantía de que la información es accesible sólo a aquellas personas autorizadas a tener acceso a ella.
Disponibilidad	Garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.
Integridad	Garantía de que se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
Autenticación	Identificación de quién hace uso de los datos o servicios
Amenaza	Sucesos que pueden materializarse causando un perjuicio a la organización
Vulnerabilidad	Posibilidad de materialización de una amenaza sobre un activo
Riesgo	Índice que integra la probabilidad de que un escenario se materialice y la degradación que supondría sobre un activo
Impacto	Índice de daño o presión al que se ve sometido un servicio, proceso o activo en caso de la materialización de una amenaza
Salvaguardas	Elementos de defensa desplegados para reducir el perjuicio para la organización en caso de materialización de una amenaza

1.3.2. ACRÓNIMOS

Acrónimo	Concepto
[D]	Disponibilidad
[I]	Integridad
[C]	Confidencialidad
UE	Unión Europea

[1] SME name and location

2. REFERENCIAS

Los siguientes documentos son aplicables en la medida que tengan carácter contractual o hayan sido aprobados por el cliente, correspondiéndose sus versiones y fechas con las vigentes en el momento de publicación del presente documento; el resto se han usado simplemente a modo de soporte.

Código	Documento
[ENISA-INF]	Paquete informativo para PYME
[MAGERITV2]	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

3. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS[2]

Hoy en día nos encontramos en un entorno en el que la información se ha convertido en uno de los principales activos de cualquier organización. Se debe entender información en un sentido amplio, independientemente de la forma en la que se guarde o se transmita. Por lo tanto, esta información debe gestionarse y protegerse estratégicamente y de forma proactiva, incluyendo los sistemas y equipos o recursos que contribuyen a su almacenamiento, proceso y transmisión.

La gestión y protección de la información crítica de la organización deber realizarse de forma inteligente, identificando los procesos de negocio, los componentes que sustentan dichos procesos y las amenazas potenciales que podrían poner en peligro la normal ejecución de los mismos. Este esfuerzo de identificación y análisis debe facilitar la toma de decisiones en cuestión de seguridad, permitiendo priorizar las actuaciones que deben realizarse y optimizar el uso de los recursos. Esta tarea de análisis para la identificación de los puntos críticos de negocio y de las principales amenazas es una práctica que debe aplicarse de forma global y sistemática en el transcurso de la actividad diaria de la organización con el fin de invertir en seguridad de una forma racional, protegiendo aquellos activos que lo necesitan y con la intensidad necesaria.

Es aquí donde entra en juego el análisis de riesgos, que pretende sistematizar todo este proceso de análisis e identificación de actividades críticas para el negocio y amenazas potenciales con el fin de estimar la magnitud de los riesgos a los que está expuesta una organización. Esto permitirá conocer el estado actual de la organización en materia de seguridad, de forma que se pueda realizar una gestión adecuada de los riesgos identificados. Esta gestión de los riesgos consistirá en la planificación e implantación de las salvaguardas adecuadas de acuerdo a los objetivos, política y estrategia de la organización con el fin de reducir, transferir o asumir dichos riesgos. El riesgo no se puede erradicará totalmente, sino que el objetivo será reducirle a un nivel residual que sea asumible para la organización.

De forma general se puede dividir el proceso de análisis de riesgos en cuatro fases diferenciadas:

1. Identificación de activos relevantes para la organización. Entendiendo activo como cualquier recurso de información o relacionado con ésta necesario para la correcta ejecución de la actividad de la organización. Es obvio que no todos los activos son iguales, sino que pertenecerán a diferentes categorías (red, hardware, software, personas, etc.), lo cual condicionará las potenciales amenazas y las salvaguardas aplicables.
2. Identificación de amenazas. Amenazas son todos aquellos sucesos que pueden ocurrir y que puede causar un perjuicio a la organización. No todas las amenazas afectan a todos los activos, sino que hay una dependencia directa entre el tipo de activo y lo que le podría ocurrir. Así, podrían extorsionar a un empleado de la organización, mientras que no ocurre lo mismo con una aplicación o un servidor. De igual forma, no todos los activos se ven afectados de igual manera ni en el mismo grado por una determinada amenaza, por lo tanto es importante estimar cómo de vulnerable es un determinado activo atendiendo a dos aspectos:
    - Degradación: Cómo de perjudicado se vería el activo ante la materialización de la amenaza. Suele expresarse como un porcentaje del valor del activo.
    - Frecuencia: Cada cuanto es probable que se materialice la amenaza. Proporciona una nueva dimensión a la degradación que puede causar una amenaza, ya que una amenaza puede ser de terribles consecuencias pero de muy probable

[2] Here comes a short description about risk analysis process for an easier understanding of the report and the concepts used on it. a short explanation about the ENISA approach is also included in this section

materialización otra podría ser de muy bajas consecuencias pero tan frecuente como para acabar acumulando un daño considerable.

Mientras que estos dos aspectos nos determinan la forma en que una amenaza puede afectar un activo, es necesario determinar en qué sentido se puede producir este perjuicio. Para ello se pueden considerar tres dimensiones en las que un activo de información podría verse afectado:

- Disponibilidad: Se debe evaluar el perjuicio de que el activo no esté o no pueda ser utilizado.
- Confidencialidad: Se debe evaluar el perjuicio de que la información sea conocida por quien no debe.
- Integridad: Se debe valorar el perjuicio de que el activo o la información pueda estar manipulada, dañada o corrupta.

3. Identificación de salvaguardas existentes. Hasta este punto no se han tenido en cuenta las salvaguardas desplegadas, se tiene por lo tanto un mapa del riesgo potencial de la organización en el que se determinan los impactos y riesgos a que estarían expuestos los activos si no se protegieran, lo cual no es habitual. Las salvaguardas pueden tener dos efectos en el riesgo presente, bien reduciendo la frecuencia o la probabilidad de que una amenaza se materialice (salvaguardas preventivas) o bien limitando el impacto producido por una amenaza. Se puede considerar una salvaguarda efectiva al 100% cuando:

   - Es teóricamente idónea
   - Está perfectamente desplegada, configurada y mantenida
   - Se emplea siempre
   - Existen procedimientos claros de uso normal y en caso de incidencias
   - Los usuarios están formados y concienciados
   - Existen controles que avisan de posibles fallos

La forma en que se relacionan todos estos elementos se muestra en la siguiente figura:

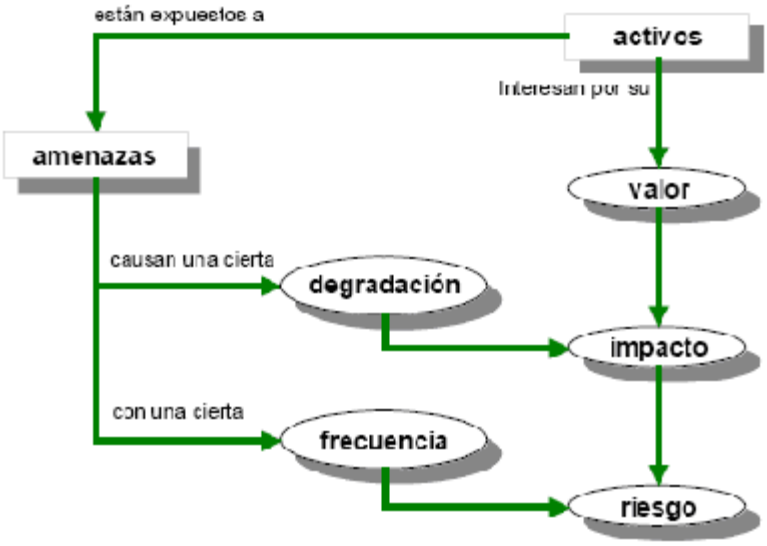

Figura 1: Relación de conceptos en el mapa de riesgos potencial

Una vez finalizado el análisis de riesgos se debe haber obtenido una visión de los impactos y riesgos residuales de la organización con las salvaguardas existentes. En el caso de que el riesgo residual no sea despreciable o asumible por la organización se tendrán que planificar y adoptar medidas que permitan alcanzar ese nivel de riesgo asumible para la organización. Es esto lo que se entiende por Gestión del Riesgo.

Durante el proceso de gestión del riesgo se deben seleccionar de forma prioritaria aquellas salvaguardas de tipo preventivo que permitan minimizar la probabilidad de que las amenazas se materialicen o que el daño producido sea despreciable. No obstante, dado que esto no es siempre posible, se deben adoptar en cualquier caso las medidas necesarias para que un posible incidente de seguridad no pase inadvertido, permitiendo su pronta detección, una reacción adecuada mediante un plan de emergencia y la posibilidad de recuperar el sistema a sus condiciones aceptables de funcionamiento lo antes posible mediante la elaboración de planes de continuidad.

Por último, debe tenerse en cuenta que una aplicación de salvaguardas eficiente debe llegar a un cierto equilibrio entre:

- Salvaguardas técnicas: en aplicaciones, equipos y comunicaciones
- Salvaguardas físicas: protegiendo el entorno de trabajo de las personas y los equipos
- Medidas de organización: de prevención y gestión de las incidencias
- Política de personal: siendo el factor humano el eslabón más débil de la seguridad, resulta de vital importancia contar con medidas adecuadas de contratación de personal, formación continua en buenas prácticas de seguridad, fomentar la participación en el reporte de incidencias y la aplicación de medidas disciplinarias cuando las normativas y política se seguridad de la organización se ven quebrantadas.

En cualquier caso se debe tener siempre presente que el punto óptimo vendrá dado por el equilibrio entre el valor del activo a proteger y la inversión realizada en salvaguardas para

protegerlo, considerando el valor del activo no sólo por su valor económico sino también en términos estratégicos, de reputación, etc.

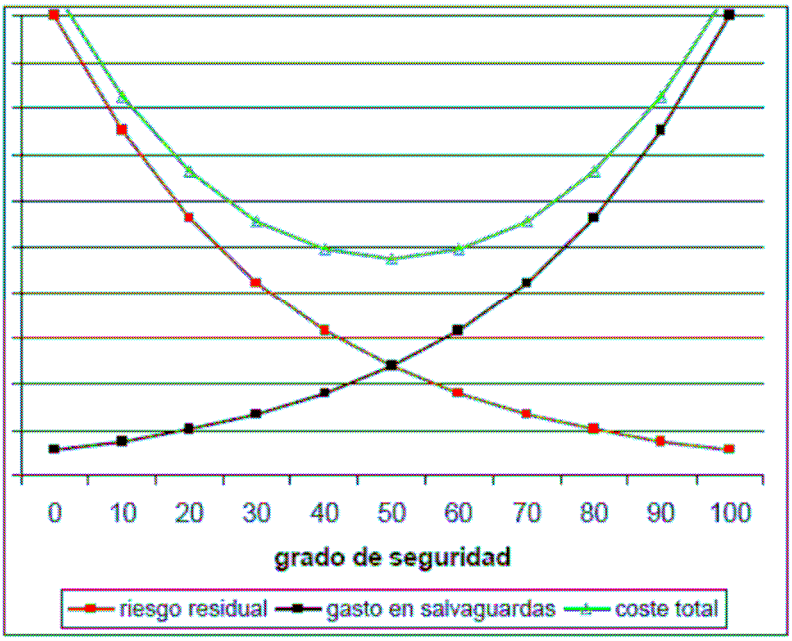

Figura 2: Grado de seguridad

En cuanto al proceso general de análisis de riesgos cabe destacar que existen diferentes metodologías que aportan diferentes enfoques a cada una de las diferentes fases que se pueden diferenciar, no obstante la mayor parte de ellas coinciden en la base conceptual y los objetivos, que han intentado plasmarse en el presente apartado.

El análisis de riesgos realizado dentro del ámbito de este piloto y cuyos resultados se expondrán en el presente documento se basa en la metodología desarrollada por ENISA. El principal objetivo de dicha metodología es la elaboración de un modelo simplificado de análisis de riesgos enfocado a pequeñas organizaciones que permita a dichas organizaciones realizar una evaluación del riesgo presente en sus entornos y seleccionar las medidas pertinentes para gestionar los riesgos identificados con un esfuerzo proporcional a sus recursos.

La metodología ENISA se basa en un enfoque en cuatro fases que tratan los siguientes aspectos:

1. Selección del perfil de riesgos: En esta fase se evalúa el perfil de riesgo de la organización mediante la utilización de un conjunto predefinido de criterios estructurados en una tabla de evaluación en la que la organización debe situarse.
2. Identificación de los activos críticos: En esta fase se seleccionan los activos más importantes en los procesos de negocio de la organización definiendo los requisitos de seguridad para cada uno de dichos activos y clasificándoles según su naturaleza.
3. Selección de tarjetas de controles o salvaguardas: Basándose en el perfil de riesgo de la organización y los requisitos de seguridad definidos para los activos de la empresa se seleccionan unos controles o salvaguardas aplicables.
4. Ejecución y gestión: Una vez determinados todos los aspectos anteriores y analizada la situación actual frente a la deseada se deben asignar prioridades en la ejecución de los controles.

Como herramienta de apoyo para aplicar la metodología se ha hecho uso de la aplicación Pilar Basic 4.3, resultado de la adaptación a la metodología ENISA de la herramienta EAR Pilar, ideada como herramienta de ayuda en la realización de los cálculos asociados al análisis de riesgos en sistemas complejos.

4. PERFIL DE RIESGO

La definición del perfil de riesgo según la metodología ENISA se realiza en base a la definición de la situación de la organización de acuerdo a las siguientes áreas y niveles:

Áreas de riesgo	Alto	Medio	Bajo
Riesgos jurídicos	La empresa maneja información de los clientes de carácter sensible y personal, incluidas historias médicas y datos personales críticos, con arreglo a lo previsto en la legislación de protección de datos de la UE	La empresa maneja la información de los clientes de índole personal, pero no sensible, conforme se define ésta en la Ley de protección de datos de la UE	La empresa no maneja datos personales distintos a los del personal empleado por ella
Riesgos de productividad	La empresa emplea a más de 100 personas que requieren a diario del acceso a aplicaciones y servicios empresariales	La empresa emplea a más de 50 personas que requieren a diario del acceso a aplicaciones y servicios empresariales	La empresa emplea a menos de 10 personas que requieren a diario del acceso a aplicaciones y servicios empresariales
Riesgos para la estabilidad financiera	Los ingresos anuales exceden de 25 millones de euros y/o las transacciones financieras con terceros o clientes tienen lugar como proceso habitual parte de su actividad empresarial	Los ingresos anuales no exceden de 25 millones de euros	Los ingresos anuales no exceden de 5 millones de euros
Riesgos para la reputación y de pérdida de confianza de los clientes	La indisponibilidad o la calidad del servicio repercuten directamente en el perfil empresarial, y/o más del 70% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa	La indisponibilidad o la calidad del servicio pueden repercutir indirectamente en el perfil empresarial, y/o menos del 5% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa	La indisponibilidad o la calidad del servicio no pueden repercutir de manera directa o indirecta en el perfil empresarial, ni derivar en pérdida de ingresos

Tabla 1: Criterios de definición del perfil de riesgos

En el caso que nos ocupa, la empresa D centra su actividad en XXXX[3]

[3] Here there come the comments over the reasons why we chose the risk profile based on the table about and the answers made to questions in the questionnaire and another one regarded with the SME business environment

Por lo tanto de acuerdo a las características de la empresa analizada y en base a los criterios definidos en la metodología ENISA de análisis de riesgos y según la percepción de la propia empresa, se pueden determinar los niveles de riesgo que se muestran en la siguiente tabla, siendo el valor más alto y el que determina el perfil de riesgo global de la empresa "**Medio**"[4]

Áreas de riesgo	Nivel de riesgo	Perfil de Riesgo
Riesgos jurídicos (*Legal and Regulatory*)	Medio (*Medium*)	Medio *(Medium)*
Riesgos de productividad (*Productivity*)	Medio (*Medium*)	
Riesgos para la estabilidad financiera (*Financial Stability*)	Medio (*Medium*)	
Riesgos para la reputación y de pérdida de confianza de los clientes (*Reputation and Loss of Customer Confidence*)	Bajo (*Low*)	

Tabla 2: Perfil de riesgo de la empresa

[4] Risk profile selection for each defined risk area

5. ACTIVOS CRÍTICOS

Tal y como se ha explicado en el apartado anterior, se han identificado dos actividades críticas para la empresa D[5]:

- XXXXXXXX
- XXXXXXXX

De forma adicional se puede destacar que la empresa dispone de portal web y servicio de correo electrónico en régimen de hosting.

Teniendo en cuenta los datos anteriores y la entrevista mantenida con los responsables de la empresa se han identificado y clasificado los siguientes activos críticos que serán incluidos en el análisis de riesgos:[6]

- Aplicaciones (*Applications*):
  - [ERP]
  - [SCADA Systems]
- Equipos (*Systems*)
  - [Archiving and Backup]
  - [Web Server, Archiving]
  - [Mail Server]
  - [workstations]
- Comunicaciones (*Network*)
  - [Cabling, routers and network segments]
  - [PABX]
- Personal (*People*)
  - [Reseach and development]
  - [Operation and technology1]
  - [Operation and technology2]
  - [Operation and technology3]
  - [IT Administrator, operation and technology]

De acuerdo a la metodología ENISA los activos enumerados pueden englobarse dentro de las siguientes categorías:[7]

[5] Critical Business activities identification

[6] Assets identification

Activo crítico (Critical Asset)	Categoría de activo (*Asset category*)	Componentes (*Components*)	Requisitos de seguridad (*Security requirements*)	Justificación de su selección (*Justification*)
Consultoría y desarrollo de proyectos (*Consulting*)	Sistemas (*Systems*)	Todos los activos definidos en este apartado	Confidencialidad (Confidentiality) Integridad (Integrity)	XXXXX

Tabla 3: Activos seleccionados

[7] Assets categorization and security requirements identification

6. SELECCIÓN DE CONTROLES

La metodología ENISA define una serie de salvaguardas organizativas y orientadas a activos que deben seleccionarse o que son recomendables según el perfil de riesgo de la empresa y los activos críticos de la misma.

Según el perfil de riesgo definido para cada una de las áreas y teniendo en cuenta las especificaciones de la metodología ENISA se pueden seleccionar los siguientes controles:[8]

Áreas de riesgo (*Risk areas*)	Nivel de riesgo (*Risk level*)	Controles organizativos (*Organizational controls*)
Riesgos jurídicos (*Legal and Regulatory*)	Medio (*Medium*)	SP1 SP4
Riesgos de productividad (*Productivity*)	Medio (*Medium*)	SP4 SP6
Riesgos para la estabilidad financiera (*Financial Stability*)	Medio (*Medium*)	SP4
Riesgos para la reputación y de pérdida de confianza de los clientes (*Reputation and Loss of Customer Confidence*)	Bajo (*Low*)	SP4.1

Tabla 4: Salvaguardas organizativas recomendadas

[8] Organizational controls

Basándonos en el perfil de riesgos global y la categorización de los activos, según la metodología ENISA se deben seleccionar los controles pertenecientes al grupo CC-2S que agrupa las siguientes salvaguardas:[9]

Identificación de la tarjeta de controles basados en los activos (*Asset Bases Control card ID*)										
	CC-2S									
Perfil de riesgos (*Risk profile*)										
	Medio									
Categoría del activo (*Asset category*)										
	Sistema									
Requisitos de seguridad (*Security requirements*)	Seguridad Física (*Physical Security*)	Gestión de sistemas y redes (*System and network Management*)	Herramientas de administración de sistemas (*System Administration tools*)	Seguimiento y auditoría de la seguridad física (*Monitoring and Auditing IT Security*)	Autenticación y autorización (*Authenticatioon and Authorization*)	Gestión de vulnerabilidades (*Vulnerability Management*)	Cifrado (*Encryption*)	Diseño y arquitectura de seguridad (*Securioty Architecture and Design*)	Gestión de incidentes (*Incident Management*)	Prácticas de personal generales (*General Staff practices*)
Confidencialidad (*Condifentiality*)		2.1.6 2.1.7			2.4.1					
Integridad (*Integrity*)		2.1.9			2.4.1					
Disponibilidad (*Availability*)		2.1.6 2.1.7								

Tabla 5: Salvaguardas orientada a activos recomendadas

[9] Score card selection and asset based controls

De esta forma se pueden concluir los siguientes controles a implantar en el sistema:

Activo	Control	Justificación de su selección
Controles basados en los activos	OP2.1.6 OP2.1.7 OP2.1.9 OP2.4.1	Los controles de autenticación y autorización, así como la realización de copias y gestión de contraseñas son de gran importancia para mantener la integridad y confidencialidad del activo objeto en consideración
Controles organizativos	SP1	Formación y sensibilización en materia de seguridad
	SP4	Política de seguridad
	SP4.1	Incluido en el SP4
	SP6	Planificación de Contingencias / recuperación en caso de catástrofe

Tabla 6: Salvaguardas recomendadas

En los siguientes aparatados del presente documento se profundiza en los aspectos incluidos en cada una de los controles recomendados, así como en el análisis entre el estado actual de implantación y el nivel recomendado de los mismos.

7. ANÁLISIS DEL ESTADO ACTUAL VS OBJETIVO

Con el objetivo de realizar una gestión y priorización adecuada de los controles seleccionados, se debe realizar un análisis que nos permita contrastar el estado actual de aplicación de las diferentes salvaguardas en la organización respecto el estado recomendable de las mismas. Para facilitar la realización de este análisis se ha dividido el grado de implantación de las salvaguardas según los siguientes niveles[10]:

- L0. La salvaguarda no se encuentra implantada en la organización.
- L1. En este nivel de madurez, las salvaguardas existen, pero no se gestionan. El éxito depende de buena suerte. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta.
- L2. En este nivel de madurez, la eficacia de las salvaguardas depende de la buena suerte y de la buena voluntad de las personas. Los éxitos son repetibles, pero no hay plan para los incidentes más allá de la reacción heroica. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.
- L3. Se despliegan y se gestionan las salvaguardas. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular de las protecciones. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece.
- L4. Usando medidas de campo, la dirección puede controlar empíricamente la eficacia y la efectividad de las salvaguardas. En particular, la dirección puede fijar metas cuantitativas de la calidad. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa, mientras que en el nivel L3, la confianza era solamente cualitativa.
- L5. Este nivel de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora de los procesos. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.

De esta forma, en las siguientes tablas se plasma para cada una de los grupos de salvaguarda la comparativa entre el estado actual y el estado objetivo o recomendable según el modelado de la metodología ENISA realizado mediante la herramienta Pilar. Las valoraciones asignadas a cada una de las salvaguardas tanto para el estado actual como el objetivo son fruto de la entrevista mantenida con la empresa y la experiencia de la empresa GMV en la realización de análisis de riesgos.

[10] Here comes by safeguard, the tables with the current situation and the regarded situation as ENISA suggests. we have done a gap analysis considering the current situation based on the meeting held with the SME. the maturity level for each control has been evaluated in six levels l0-l5 in order to simplify the gap analysis.

For each table with the safeguards and the evaluation, we have made comments with the justification or any finding that echoes the evidence if required.

[SP1] Formación y sensibilización en materia de seguridad

salvaguarda	[presente]	[objetivo]
[SP1.1] Los miembros del personal comprenden sus funciones y responsabilidades en materia de seguridad. Este hecho está documentado y comprobado.	L1	L3
[SP1.2] Se dispone de conocimientos técnicos internos adecuados para la totalidad de servicios, mecanismos y tecnologías empleados (p. ej., registro, seguimiento o codificación), incluido el funcionamiento de éstos en condiciones de seguridad. Este hecho está documentado y comprobado.	L2	L3
[SP1.3] Se imparten a todo el personal conocimientos y formación y se le envían recordatorios periódicos en materia de seguridad. El conocimiento del personal está documentado, y la conformidad se comprueba periódicamente. La formación comprende los temas que siguen:	L1	L3
estrategias, metas y objetivos en materia de seguridad	L1	L3
reglamentos, políticas y procedimientos de seguridad	L1	L3
políticas y procedimientos de colaboración con terceros	L1	L3
planes para contingencias y recuperación en caso de catástrofe	L1	L3
requisitos relativos a la seguridad física	L1	L3
perspectiva de los usuarios respecto a	L1	L3
la gestión de sistemas y redes	L1	L3
las herramientas de administración del sistema	L1	L3
el seguimiento y la auditoría en lo que atañe a la seguridad física y asociada a las tecnologías de la información	L1	L3
autenticación y autorización	L1	L3
gestión de vulnerabilidades	L1	L3
codificación	L1	L3
arquitectura y diseño	L1	L3
gestión de incidentes	L1	L3
prácticas generales de personal	L1	L3
observancia de la legislación, sanciones y actuaciones disciplinarias por infracciones de la seguridad	L1	L3
modo de acceder correctamente a la información sensible y trabajo en las áreas en las que ésta es accesible	L1	L3
políticas y procedimientos de extinción de la relación laboral en lo que atañe a la seguridad	L1	L3

Comentarios:[11]

[11] Regarded comments. Example: Staff members apply common security practices based on their own knowledge. These practices are not documented or linked with internal policy or employee's contracts.

Organization common security practices should be documented and included in the internal training program. In addition, staff members should sign non disclosure agreements at the beginning of working relationship. …

[SP4] Políticas y normativas de seguridad

salvaguarda	[presente]	[objetivo]
[SP4.1] La organización dispone de un conjunto exhaustivo de políticas vigentes y documentadas que se revisan y actualizan periódicamente. Estas políticas abordan áreas temáticas fundamentales en materia de seguridad, entre las que se cuentan:	L0	L2
la gestión y la estrategia de seguridad	L1	L2
la gestión de riesgos para la seguridad	L1	L2
la seguridad física	L1	L2
la gestión de sistemas y redes	L2	L2
las herramientas de administración de sistemas	L2	L2
el seguimiento y la auditoría	L1	L2
la autenticación y la autorización	L2	L2
la gestión de vulnerabilidades	L0	L2
la codificación	L1	L2
la arquitectura y el diseño de la seguridad	L2	L2
la gestión de incidentes	L1	L2
las prácticas de seguridad de personal	L1	L2
la legislación aplicable	L1	L2
la sensibilización y la formación	L1	L2
la seguridad de la información basada en la colaboración	L1	L2
la planificación de contingencias y la recuperación en caso de catástrofe	L1	L2
[SP4.2] Existe un proceso documentado para la gestión de políticas de seguridad, incluidas las tareas de:	L3	L3
creación	L3	L3
administración (incluidas revisiones y actualizaciones periódicas)	L3	L3
comunicación	L3	L3
[SP4.3] La organización cuenta con un proceso documentado para la evaluación periódica (técnica y no técnica) del cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L2	L3
[SP4.4] La organización cuenta con un proceso documentado para garantizar el cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L2	L3
[SP4.5] La organización aplica de manera uniforme sus políticas de seguridad.	L1	L3
[SP4.6] Únicamente el personal autorizado puede comprobar y revisar las políticas y procedimientos de seguridad.	L3	L3

Comentarios:

[SP6] Planificación de contingencias / recuperación en caso de catástrofe

salvaguarda	[presente]	[objetivo]
[SP6.1] Se ha efectuado un análisis de operaciones, aplicaciones y de la significación de los datos.	L3	L3
[SP6.2] La organización ha documentado	L3	L3
los planes de continuidad de la actividad empresarial y de operación en casos de emergencia	L3	L3
los planes de recuperación en caso de catástrofe	L3	L3
los planes de contingencia para la respuesta en casos de emergencia	L3	L3
[SP6.3] En los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial se consideran los	L3	L3

requisitos y conrtroles de acceso físico y electrónico.		
[SP6.4] Los planes de contingencia, recuperación en caso de catástrofe, y continuidad de la actividad empresarial se revisan y comprueban periódicamente.	L3	L3
[SP6.5] Todo el personal ...	L3	L3
tiene conocimiento de los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial	L3	L3
comprende sus responsabilidades y está capacitado para cumplirlas	L3	L3

Comentarios

[OP2] Seguridad de las tecnologías de la información

salvaguarda	[presente]	[objetivo]
[OP2.1.6] Existe un plan de copias de respaldo de datos que	L2	L2
se actualiza regularmente	L2	L2
se comprueba periódicamente	L2	L2
requiere la realización de copias de respaldo programadas regularmente, tanto del software, como de los datos	L2	L2
requiere la comprobación y verificación periódicas de la capacidad para restaurar a partir de copias de respaldo	L2	L2
[OP2.1.7] Todo el personal comprende y es capaz de desempeñar sus responsabilidades con arreglo a los planes de respaldo.	L2	L3
[OP2.1.9] Los miembros del personal de TI siguen los procedimientos pertinentes al publicar, modificar y anular contraseñas, cuentas y privilegios de usuario.	L2	L2
Se requiere una identificación única de usuario para todos los usuarios del sistema de información, incluidos los usuarios terceros.	L2	L2
Las cuentas y contraseñas por defecto han sido suprimidas de los sistemas.	L2	L2
[OP2.4] Autenticación y autorización	L0	L3
[OP2.4.1] Se utilizan controles de acceso y mecanismos de autenticación de usuario apropiados (p. ej., permisos de archivo, configuración de red) coherentes con la política establecida al respecto, con el fin de restringir el acceso de los usuarios a	L1	L3
la información	L3	L3
las utilidades del sistema	L2	L3
el código fuente de programas	n.a.	n.a.
los sistemas sensibles	L2	L3
determinadas aplicaciones y servicios	L1	L3
conexiones de red en la organización	L2	L3
conexiones de red con origen fuera de la organización	L2	L3

Comentarios

8. RESUMEN EJECUTIVO

XXXXX[12]

[12] Here comes the most important aspects and recommendations that the SME should take into account with regard to ENISA risk analysis approach and GMV expertise. it includes recommendations about the selected scorecards in ENISA methodology and other relevants aspects

9. ANEXO A: RESULTADOS DE LA HERRAMIENTA PILAR

La herramienta Pilar permite completar los resultados de la metodología ENISA con consideraciones más específicas de análisis de riesgos, enriqueciendo los resultados obtenidos con datos más específicos y gráficos que permiten contrastar de forma rápida y sencilla la evolución del riesgo en la organización respecto al grado de implantación de las salvaguardas.

En cuanto a la selección de amenazas, la herramienta Pilar permite definir las amenazas de interés para cada uno de los activos. Cada una de estas amenazas tendrá asociados unos parámetros de impacto para cada una de las dimensiones de seguridad en caso de materialización y frecuencia de ocurrencia. En la versión utilizada de la herramienta para el desarrollo del piloto, se seleccionan unas amenazas por defecto para cada tipo de activo según su naturaleza, personas, red, hardware, ..., con valores también por defecto para la frecuencia y el impacto. Esto permite al usuario abstraerse de la complejidad asociada a la selección de este tipo de parámetros durante el análisis de riesgos a la vez que se permite desglosar la información del mapa de riesgo por cada una de las amenazas asociadas a los activos. De forma complementaria a las amenazas seleccionadas por defecto la herramienta permite seleccionar amenazas adicionales que permitan adaptarse a los diferentes requisitos del sector de actividad de cada empresa. Las amenazas por defecto para cada uno de los activos que han sido seleccionadas en la herramienta son las siguientes:

Aplicaciones
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.19] Escapes de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.14] Interceptación de información (escucha)
[A.22] Manipulación de programas

Tabla 7: Amenazas de aplicaciones

Equipos
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico

[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.19] Escapes de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.14] Interceptación de información (escucha)
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo

Tabla 8: Amenazas de equipos

Comunicaciones
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia

[E.19] Escapes de información
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.14] Interceptación de información (escucha)
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo

Tabla 9: Amenazas de comunicaciones

Personas
[E.7] Deficiencias en la organización
[E.19] Escapes de información
[E.28] Indisponibilidad del personal
[A.19] Divulgación de información
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)

Tabla 10: Amenazas de personas

En cuanto al mapa de riesgos, la herramienta permite representar de forma gráfica el riesgo presente en la organización en diferentes momentos en función del estado de implantación de las salvaguardas en dichos momentos. En el desarrollo del piloto se han analizado las siguientes estados:[13]

- Riesgo potencial: Riesgo en caso de no existir implantada ninguna salvaguarda.
- Riesgo presente: Riesgo existente en la organización con el estado de implantación actual de las salvaguardas.
- Riesgo objetivo: Riesgo existente en la organización si se implantasen las salvaguardas recomendadas por la metodología ENISA y aquellas recomendaciones fruto de la experiencia de la empresa GMV y los aspectos analizados durante las entrevistas mantenidas con la empresa.

Cada uno de estos mapas de riesgo pueden observarse en las siguientes figuras.

[13] Here comes the potential risk, current risk and target risk images obtained from pilar tool for each SME.

activo	[D]	[I]	[C]
ACTIVOS	{6.3}	{6.3}	{6.3}
[SW] Aplicaciones	{5.9}	{6.3}	{6.3}
[redacted]	{5.9}	{6.3}	{6.3}
[redacted]	{5.9}	{6.3}	{6.3}
[HW] Equipos	{6.3}	{6.3}	{6.3}
[redacted]	{6.3}	{5.6}	{5.6}
[redacted]	{6.3}	{6.3}	{6.3}
[redacted]	{6.3}	{6.3}	{6.3}
[redacted]	{6.3}	{6.3}	{6.3}
[COM] Comunicaciones	{5.9}	{3.3}	{5.3}
[redacted]	{5.9}	{3.3}	{5.3}
[redacted]	{5.6}	{3.3}	{5.3}
[P] Personal	{4.3}	{4.9}	{5.0}
[redacted]	{4.3}	{4.9}	{5.0}
[redacted]	{4.3}	{4.9}	{5.0}
[redacted]	{4.3}	{4.9}	{5.0}
[redacted]	{4.3}	{4.9}	{5.0}
[redacted]	{4.3}	{4.9}	{5.0}

Figura 3: Riesgo potencial

activo	[D]	[I]	[C]
ACTIVOS	{3.7}	{3.6}	{3.6}
[SW] Aplicaciones	{3.3}	{3.6}	{3.6}
[redacted]	{3.3}	{3.6}	{3.6}
[redacted]	{3.3}	{3.6}	{3.6}
[HW] Equipos	{3.7}	{3.6}	{3.6}
[redacted]	{3.7}	{3.0}	{2.9}
[redacted]	{3.6}	{3.6}	{3.6}
[redacted]	{3.7}	{3.6}	{3.6}
[redacted]	{3.7}	{3.6}	{3.6}
[COM] Comunicaciones	{3.4}	{0.8}	{2.8}
[redacted]	{3.4}	{0.8}	{2.8}
[redacted]	{3.1}	{0.8}	{2.8}
[P] Personal	{1.6}	{2.2}	{2.4}
[redacted]	{1.6}	{2.2}	{2.4}
[redacted]	{1.6}	{2.2}	{2.4}
[redacted]	{1.6}	{2.2}	{2.4}
[redacted]	{1.6}	{2.2}	{2.4}
[redacted]	{1.6}	{2.2}	{2.4}

Figura 4: Riesgo Presente

activo	[D]	[I]	[C]
ACTIVOS	{1.6}	{1.5}	{1.5}
[SW] Aplicaciones	{1.3}	{1.5}	{1.5}
[redacted]	{1.3}	{1.5}	{1.5}
[redacted]	{1.3}	{1.5}	{1.5}
[HW] Equipos	{1.6}	{1.4}	{1.5}
[redacted]	{1.6}	{0.8}	{0.9}
[redacted]	{1.6}	{1.4}	{1.5}
[redacted]	{1.6}	{1.4}	{1.5}
[redacted]	{1.6}	{1.4}	{1.5}
[COM] Comunicaciones	{1.2}	{0.0}	{0.5}
[redacted]	{1.2}	{0.0}	{0.5}
[redacted]	{0.9}	{0.0}	{0.5}
[P] Personal	{0.0}	{0.4}	{0.5}
[redacted]	{0.0}	{0.4}	{0.5}
[redacted]	{0.0}	{0.4}	{0.5}
[redacted]	{0.0}	{0.4}	{0.5}
[redacted]	{0.0}	{0.4}	{0.5}
[redacted]	{0.0}	{0.4}	{0.5}

Figura 5: Riesgo objetivo

En el proyecto de la herramienta Pilar proporcionado a la empresa se pueden desglosar cada uno de los mapas de riesgo anteriores en función de las distintas amenazas.

Adicionalmente, el análisis completo de implantación de salvaguardas que se ha tenido en cuenta para la obtención de los mapas de riesgo anteriores se presenta en el Anexo B del presente documento.

10. ANEXO B: ESTADO DE IMPLANTACIÓN DE SALVAGUARDAS[14]

[SP1] Formación y sensibilización en materia de seguridad

salvaguarda	[presente]	[objetivo]
[SP1.1] Los miembros del personal comprenden sus funciones y responsabilidades en materia de seguridad. Este hecho está documentado y comprobado.	L1	L3
[SP1.2] Se dispone de conocimientos técnicos internos adecuados para la totalidad de servicios, mecanismos y tecnologías empleados (p. ej., registro, seguimiento o codificación), incluido el funcionamiento de éstos en condiciones de seguridad. Este hecho está documentado y comprobado.	L2	L3
[SP1.3] Se imparten a todo el personal conocimientos y formación y se le envían recordatorios periódicos en materia de seguridad. El conocimiento del personal está documentado, y la conformidad se comprueba periódicamente. La formación comprende los temas que siguen:	L1	L3
estrategias, metas y objetivos en materia de seguridad	L1	L3
reglamentos, políticas y procedimientos de seguridad	L1	L3
políticas y procedimientos de colaboración con terceros	L1	L3
planes para contingencias y recuperación en caso de catástrofe	L1	L3
requisitos relativos a la seguridad física	L1	L3
perspectiva de los usuarios respecto a	L1	L3
la gestión de sistemas y redes	L1	L3
las herramientas de administración del sistema	L1	L3
el seguimiento y la auditoría en lo que atañe a la seguridad física y asociada a las tecnologías de la información	L1	L3
autenticación y autorización	L1	L3
gestión de vulnerabilidades	L1	L3
codificación	L1	L3
arquitectura y diseño	L1	L3
gestión de incidentes	L1	L3
prácticas generales de personal	L1	L3
observancia de la legislación, sanciones y actuaciones disciplinarias por infracciones de la seguridad	L1	L3
modo de acceder correctamente a la información sensible y trabajo en las áreas en las que ésta es accesible	L1	L3
políticas y procedimientos de extinción de la relación laboral en lo que atañe a la seguridad	L1	L3

Comentarios

[SP2] Estrategia de seguridad

[14] Here comes by safeguard, the tables with the current situation and the target situation. in this section, we have included the gap analisys for safeguards not suggested by ENISA approach but GMV consider that are important controls to take into account by the SME.

salvaguarda	[presente]	[objetivo]
[SP2.1] Las estrategias empresariales de la organización incorporan de manera rutinaria consideraciones de seguridad.	L1	L2
[SP2.2] En las estrategias y políticas de seguridad se tienen en cuenta las estrategias y objetivos empresariales de la organización.	L1	L2
[SP2.3] Las estrategias, metas y objetivos en materia de seguridad se documentan y se revisan, actualizan y comunican periódicamente a la organización.	L1	L2

Comentarios

[SP3] Gestión de seguridad

salvaguarda	[presente]	[objetivo]
[SP3.1] La dirección asigna fondos y recursos suficientes a las actividades de seguridad de la información.	L2	L2
[SP3.2] Se definen funciones y responsabilidades en materia de seguridad para todo el personal de la organización.	L1	L1
[SP3.3] En las prácticas de la organización en materia de contratación y de extinción de la relación laboral con el personal se tienen en cuenta las cuestiones de seguridad de la información.	L3	L3
[SP3.4] Los niveles requeridos de seguridad de la información y el modo en que se aplican a personas y grupos se documentan y aplican.	L1	L1
[SP3.5] La organización gestiona los riesgos que atañen a la seguridad de la información, con inclusión de:	L1	L2
la evaluación de los riesgos para la seguridad de la información, tanto periódicamente, como en respuesta a cambios significativos en la tecnología, amenazas internas o externas, o los sistemas y operaciones de la organización	L1	L2
la adopción de medidas para mitigar los riesgos hasta alcanzar un nivel aceptable	L1	L2
el mantenimiento de un nivel de riesgos aceptable	L1	L2
la utilización de evaluaciones de riesgos para la seguridad de la información con el fin de facilitar la selección de medidas de seguridad y control rentables, equilibrando los costes de ejecución con las posibles pérdidas	L1	L2
[SP3.6] La dirección recibe informes rutinarios, y actúa basándose en ellos, en los que se resumen los resultados de:	L0	L2
la revisión de los registros de sistema	L0	L2
la revisión de los historiales de auditoría	L0	L2
las evaluaciones de vulnerabilidades tecnológicas	L0	L2
los incidentes de seguridad y las respuestas dadas a los mismos	L0	L2
las evaluaciones de riesgos	L0	L2
las revisiones de la seguridad física	L0	L2
los planes y recomendaciones para la mejora de la seguridad	L0	L2

Comentarios

[SP4] Políticas y normativas de seguridad

salvaguarda	[presente]	[objetivo]
[SP4.1] La organización dispone de un conjunto exhaustivo de políticas vigentes y documentadas que se revisan y actualizan periódicamente. Estas políticas abordan áreas temáticas fundamentales en materia de seguridad, entre las que se cuentan:	L0	L2

la gestión y la estrategia de seguridad	L1	L2
la gestión de riesgos para la seguridad	L1	L2
la seguridad física	L1	L2
la gestión de sistemas y redes	L2	L2
las herramientas de administración de sistemas	L2	L2
el seguimiento y la auditoría	L1	L2
la autenticación y la autorización	L2	L2
la gestión de vulnerabilidades	L0	L2
la codificación	L1	L2
la arquitectura y el diseño de la seguridad	L2	L2
la gestión de incidentes	L1	L2
las prácticas de seguridad de personal	L1	L2
la legislación aplicable	L1	L2
la sensibilización y la formación	L1	L2
la seguridad de la información basada en la colaboración	L1	L2
la planificación de contingencias y la recuperación en caso de catástrofe	L1	L2
[SP4.2] Existe un proceso documentado para la gestión de políticas de seguridad, incluidas las tareas de:	L3	L3
creación	L3	L3
administración (incluidas revisiones y actualizaciones periódicas)	L3	L3
comunicación	L3	L3
[SP4.3] La organización cuenta con un proceso documentado para la evaluación periódica (técnica y no técnica) del cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L2	L3
[SP4.4] La organización cuenta con un proceso documentado para garantizar el cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.	L2	L3
[SP4.5] La organización aplica de manera uniforme sus políticas de seguridad.	L1	L3
[SP4.6] Únicamente el personal autorizado puede comprobar y revisar las políticas y procedimientos de seguridad.	L3	L3

Comentarios

[SP5] Gestión de la seguridad en régimen de colaboración

salvaguarda	[presente]	[objetivo]
[SP5.1] La organización ha procedido a la documentación, el seguimiento y la ejecución de procedimientos para la protección de su información cuando colabora con entidades externas (p. ej., terceros, colaboradores, subcontratistas o socios).	L2	L2
[SP5.2] La organización ha comprobado que los servicios, mecanismos y tecnologías de seguridad externalizados satisfacen sus necesidades y requisitos.	L2	L2
[SP5.3] La organización documenta, supervisa y aplica estrategias de protección de la información perteneciente a entidades externas a la que se accede desde componentes de su infraestructura, o que es utilizada por su personal.	L2	L2
[SP5.4] La organización ofrece y verifica actividades de sensibilización y formación sobre las políticas y los procedimientos de seguridad de entidades externas para el personal que interactúa con éstas.	L1	L1
[SP5.5] Existen procedimientos documentados respecto al personal	L2	L2

externo cuya relación con la organización ha concluido, en los que se especifican las medidas de seguridad pertinentes para finalizar su posibilidad de acceso. Estos procedimientos se comunican a la organización externa y se coordinan con ella.		

[SP6] Planificación de contingencias / recuperación en caso de catástrofe

salvaguarda	[presente]	[objetivo]
[SP6.1] Se ha efectuado un análisis de operaciones, aplicaciones y de la significación de los datos.	L3	L3
[SP6.2] La organización ha documentado	L3	L3
los planes de continuidad de la actividad empresarial y de operación en casos de emergencia	L3	L3
los planes de recuperación en caso de catástrofe	L3	L3
los planes de contingencia para la respuesta en casos de emergencia	L3	L3
[SP6.3] En los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial se consideran los requisitos y conrtroles de acceso físico y electrónico.	L3	L3
[SP6.4] Los planes de contingencia, recuperación en caso de catástrofe, y continuidad de la actividad empresarial se revisan y comprueban periódicamente.	L3	L3
[SP6.5] Todo el personal ...	L3	L3
tiene conocimiento de los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial	L3	L3
comprende sus responsabilidades y está capacitado para cumplirlas	L3	L3

Comentarios

[OP1] Seguridad física

salvaguarda	[presente]	[objetivo]
[OP1.1] Planes y procedimientos de seguridad física	L2	L2
[OP1.1.1] Existen planes de seguridad de las instalaciones documentados, concebidos para salvaguardar locales, edificios y cualquier otra área restringida.	L2	L2
[OP1.1.2] Estos planes se revisan, comprueban y actualizan periódicamente.	L2	L2
[OP1.1.3] Los procedimientos y mecanismos de seguridad física se comprueban y revisan periódicamente.	L2	L2
[OP1.1.4] Existen políticas y procedimientos documentados para la gestión de visitantes, que incluyen	L3	L2
el registro en la entrada	L3	L2
el acompañamiento por las instalaciones	L3	L2
los registros de acceso	L3	L2
la recepción y los servicios de hospitalidad	L3	L2
[OP1.1.5] Existen políticas y procedimientos documentados para el control físico del hardware y el software, incluidos	L1	L2
terminales, portátiles, módem, componentes inalámbricos y todos los demás elementos utilizados para acceder a la información	L1	L2
el acceso, el almacenamiento y la recuperación de copias de seguridad de datos	L1	L2

el almacenamiento de información sensible en medios físicos y electrónicos	L1	L2
la supresión de información sensible, o de los medios en los que se encuentra almacenada	L1	L2
la reutilización y el reciclaje de papel y medios electrónicos.	L1	L2
[OP1.2] Control de acceso físico	L2	L3
[OP1.2.1] Existen políticas y procedimientos documentados respecto al acceso individual y en grupo, que comprenden:	L3	L3
las normas de concesión del nivel pertinente de acceso físico	L3	L3
las normas para la determinación de los derechos iniciales de acceso	L3	L3
la modificación del derecho de acceso	L3	L3
la anulación del derecho de acceso	L3	L3
la revisión y la comprobación periódicas de los derechos de acceso	L3	L3
[OP1.2.2] Existen políticas, procedimientos y mecanismos documentados para controlar el acceso físico a entidades definidas. Se incluyen aquí:	L2	L3
áreas de trabajo	L2	L3
medios de hardware (ordenadores, dispositivos de comunicación, etc.) y de software	L2	L3
[OP1.2.3] Existen procedimientos documentados para verificar la autorización de acceso antes de autorizar el acceso físico.	L2	L3
[OP1.2.4] Los terminales y otros componentes que permiten el acceso a información sensible se encuentran físicamente protegidos con el fin de evitar accesos no autorizados.	L3	L3
[OP1.3] Seguimiento y auditoría de la seguridad física	L2	L3
[OP1.3.1] Se conservan registros de mantenimiento para documentar las reparaciones y modificaciones de los componentes físicos de las instalaciones.	L2	L3
[OP1.3.2] Pueden justificarse las acciones de una persona o de un grupo respecto a la totalidad de medios controlados físicamente.	L2	L3
[OP1.3.3] Se examinan regularmente registros de auditoría y seguimiento para detectar anomalías, y se emprenden acciones correctivas en caso necesario.	L2	L3

Comentarios

[OP2] Seguridad de las tecnologías de la información

salvaguarda	[presente]	[objetivo]
[OP2.1] Gestión de sistemas y redes	L0	L2
[OP2.1.1] Existen planes de seguridad documentados para la salvaguarda de sistemas y redes.	L1	L3
[OP2.1.2] Los planes de seguridad se revisan, comprueban y actualizan periódicamente.	L0	L2
[OP2.1.3] Se protege la información sensible mediante su almacenamiento en condiciones de seguridad, como el que proporcionan	L3	L2
las cadenas de custodia definidas	L3	L2
las copias de respaldo almacenadas fuera de las instalaciones	L3	L2
los medios de almacenamiento separables	L3	L2
un proceso de eliminación de la información sensible o de sus medios de almacenamiento	L3	L2
[OP2.1.4] La integridad del software instalado se verifica regularmente.	L0	L3

[OP2.1.5] Todos los sistemas se encuentran actualizados respecto a revisiones, parches, y recomendaciones en documentos de asesoramiento sobre seguridad.	L2	L3
[OP2.1.6] Existe un plan de copias de respaldo de datos que	L2	L2
se actualiza regularmente	L2	L2
se comprueba periódicamente	L2	L2
requiere la realización de copias de respaldo programadas regularmente, tanto del software, como de los datos	L2	L2
requiere la comprobación y verificación periódicas de la capacidad para restaurar a partir de copias de respaldo	L2	L2
[OP2.1.7] Todo el personal comprende y es capaz de desempeñar sus responsabilidades con arreglo a los planes de respaldo.	L2	L3
[OP2.1.8] Los cambios del hardware y el software de las TI se planifican, supervisan y documentan.	L1	L3
[OP2.1.9] Los miembros del personal de TI siguen los procedimientos pertinentes al publicar, modificar y anular contraseñas, cuentas y privilegios de usuario.	L2	L2
Se requiere una identificación única de usuario para todos los usuarios del sistema de información, incluidos los usuarios terceros.	L2	L2
Las cuentas y contraseñas por defecto han sido suprimidas de los sistemas.	L2	L2
[OP2.1.10] Sólo operan en los sistemas los servicios necesarios; todos los innecesarios se han suprimido.	L1	L3
[OP2.2] Herramientas de administración de sistemas	L0	L2
[OP2.2.1] Los nuevos instrumentos de seguridad, procedimientos y mecanismos se revisan de manera ordinaria para determinar su aplicabilidad en la consecución de las estrategias de seguridad de la organización.	L1	L2
[OP2.2.2] Las herramientas y los mecanismos para conseguir el uso de una administración de sistemas y de red segura, y su revisión y actualización o sustitución con carácter periódico. Son ejemplos de estas herramientas los que siguen:	L0	L2
comprobadores de la integridad de los datos	L1	L2
herramientas de codificación	L1	L2
escáneres de vulnerabilidades	L0	L2
herramientas de comprobación de la calidad de las contraseñas	L1	L2
escáneres de virus	L2	L2
herramientas de gestión de procesos	L1	L2
sistemas de detección de intrusos	L0	L2
administraciones remotas seguras	L0	L2
herramientas de servicio de red	L1	L2
analizadores de tráfico	L1	L2
herramientas de respuesta en caso de incidente	L1	L2
herramientas forenses para el análisis de datos	L1	L2
[OP2.3] Seguimiento y auditoría de la seguridad física	L0	L2
[OP2.3.1] La organización utiliza de manera ordinaria herramientas de seguimiento y auditoría de sistemas y redes.	L1	L2
La actividad es objeto de seguimiento por parte del personal de TI.	L1	L2
Se registra la actividad de sistemas y redes.	L2	L2
Los registros se revisan regularmente.	L1	L2
La actividad inusual se trata con arreglo a la política o el procedimiento pertinentes.	L1	L2
Las herramientas se revisan y actualizan periódicamente.	L1	L2

[OP2.3.2] Los cortafuegos y otros componentes de seguridad se auditan periódicamente para determinar su conformidad con la política pertinente.	L0	L2
[OP2.4] Autenticación y autorización	L0	L3
[OP2.4.1] Se utilizan controles de acceso y mecanismos de autenticación de usuario apropiados (p. ej., permisos de archivo, configuración de red) coherentes con la política establecida al respecto, con el fin de restringir el acceso de los usuarios a	L1	L3
la información	L3	L3
las utilidades del sistema	L2	L3
el código fuente de programas	n.a.	n.a.
los sistemas sensibles	L2	L3
determinadas aplicaciones y servicios	L1	L3
conexiones de red en la organización	L2	L3
conexiones de red con origen fuera de la organización	L2	L3
[OP2.4.2] Existen políticas y procedimientos de uso de la información documentados respecto al acceso individual y en grupo con el fin de:	L2	L3
establecer las normas de concesión del nivel pertinente de acceso	L2	L3
establecer un derecho inicial de acceso	L2	L3
modificar el derecho de acceso	L2	L3
anular el derecho de acceso	L2	L3
revisar y comprobar periódicamente los derechos de acceso	L2	L3
[OP2.4.3] Los métodos y mecanismos de control de acceso restringen el acceso a los recursos con arreglo a los derechos determinados en políticas y procedimientos.	L2	L4
[OP2.4.4] Los métodos y mecanismos de control de acceso se revisan y comprueban periódicamente.	L1	L3
[OP2.4.5] Se dotan métodos o mecanismos para garantizar que la información sensible no es objeto de acceso, alteración o destrucción de un modo no autorizado.	L2	L3
[OP2.4.6] Se utilizan mecanismos de autenticación para proteger la disponibilidad, integridad y confidencialidad de la información sensible. Son ejemplos de estos instrumentos los que siguen:	L0	L3
las firmas digitales	L0	L3
la biometría	L0	L3
[OP2.5] Gestión de vulnerabilidades	L0	L2
[OP2.5.1] Existe un conjunto documentado de procedimientos para la gestión de vulnerabilidades, entre los que figuran:	L0	L2
la selección de herramientas de evaluación de vulnerabilidades, listas de comprobación y scripts	L0	L2
el mantenimiento al día respecto a los tipos de vulnerabilidades conocidos y los métodos de ataque	L0	L2
la revisión de fuentes de información sobre anuncios de vulnerabilidad, alertas de seguridad y notificaciones	L0	L2
la identificación de componentes de infraestructura para su evaluación	L0	L2
la programación de evaluaciones de vulnerabilidad	L0	L2
la interpretación de resultados y la respuesta a éstos	L0	L2
el mantenimiento de un almacenamiento seguro y la disposición de datos sobre vulnerabilidad	L0	L2
[OP2.5.2] Los procedimientos de gestión de vulnerabilidades son objeto de seguimiento, así como de revisiones y actualizaciones periódicas.	L0	L2

[OP2.5.3] Las evaluaciones de vulnerabilidad de la tecnología se realizan de manera periódica, y las vulnerabilidades se tratan cuando se detectan.	L0	L3
[OP2.6] Codificación	L1	L3
[OP2.6.1] Se utilizan controles de seguridad apropiados para proteger la información sensible durante su almacenamiento o transmisión, incluidos	L2	L3
el cifrado de datos durante la transmisión	L2	L3
el cifrado de datos al escribir en disco	L2	L3
el uso de infraestructura de claves públicas	L2	L3
la tecnología de redes privadas virtuales	L2	L3
el cifrado de todas las transmisiones a través de Internet	L2	L3
[OP2.6.2] Se utilizan protocolos cifrados cuando se gestionan de manera remota sistemas, enrutadores y cortafuegos	L2	L3
[OP2.6.3] Los controles y protocolos de cifrado se someten a revisiones y comprobaciones periódicas	L1	L3
[OP2.7] Diseño y arquitectura de seguridad	L2	L2
[OP2.7.1] En la arquitectura y el diseño de sistemas nuevos y revisados se tienen en cuenta	L2	L2
las estrategias, políticas y procedimientos de seguridad	L2	L2
el historial de situaciones de riesgo en materia de seguridad	L3	L2
los resultados de las evaluaciones de riesgos para la seguridad	L2	L2
[OP2.7.2] La organización dispone de diagramas actualizados que muestren la tipología de red y la arquitectura de seguridad del conjunto de la empresa.	L3	L3

Comentarios

[OP3] Seguridad del personal

salvaguarda	[presente]	[objetivo]
[OP3.1] Gestión de incidentes	L1	L3
[OP3.1.1] Existen procedimientos documentados para la identificación de presuntos incidentes e infracciones de seguridad, así como para la elaboración de informes al respecto, y para la adopción de respuestas a los mismos, entre los que figuran:	L1	L3
los incidentes que atañen a las redes	L1	L3
los incidentes relativos al acceso físico	L1	L3
los incidentes de ingeniería social	L1	L3
[OP3.1.2] Los procedimientos de gestión de incidentes se comprueban, verifican y actualizan periódicamente.	L1	L3
[OP3.1.3] Existen políticas y procedimientos documentados respecto a la colaboración con los órganos encargados de velar por el cumplimiento de las leyes.	L1	L3
[OP3.2] Prácticas de personal generales	L1	L2
[OP3.2.1]Los miembros del personal se atienen a buenas prácticas en materia de seguridad, como las que siguen:	L2	L2
asegurar la información respecto a la que son responsables	L2	L2
abstenerse de divulgar información sensible a terceros (resistencia a la ingeniería social)	L2	L2
disponer de la capacidad adecuada para utilizar los equipos y el software de las tecnologías de la información	L2	L2
utilizar buenas prácticas en lo que se refiere a las contraseñas	L2	L2
comprender y observar las políticas y reglamentos de seguridad	L2	L2

reconocer los incidentes e informar de éstos	L2	L2
[OP3.2.2] Todo el personal, a todas las escalas de responsabilidad, desempeña las funciones que se le han asignado y asume sus responsabilidades en lo que atañe a la seguridad de la información.	L1	L3
[OP3.2.3] Existen procedimientos documentados para autorizar y supervisar a aquéllos que manejan información sensible o trabajan en emplazamientos en los que se deposita la misma. Se trata de:	L2	L2
empleados	L2	L2
contratistas, socios, colaboradores, y personal de entidades terceras	L2	L2
personal de mantenimiento de sistemas	L2	L2
personal de mantenimiento de instalaciones	L2	L2

Comentarios