ANNEX 1 - MATRIX

Initiating Process Group

4.1 Develop Project Charter

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					**1**	- No mention in the ISO documentation
Present in the proyect			x			**3**	- Declaration by the top management including IS values in the organizations core objectives - Although there is not an official document, the responsibility/authority unofficially fell upon the head of the IT department who assumed it instantly

13.1 Identify Stakeholders

	1	2	3	4	5	Score	Comments
Present in ISO 27001				x		**4**	- The ISO 27001 stablishes the importance of having the support of the top management - The ISO 27001 does not consider the impact that other stakeholders may have
Present in the proyect					x	**5**	- Once the information security risks inventory was completed, all risk owners were identified. - Responsibility for a particular risk could change after further evaluation but no risk could be registered in the initial inventory without being assigned to a particular stakeholder

Planning Process Group

4.2 Develop Project Management Plan

	1	2	3	4	5	Score	Comments
Present in ISO 27001			x			**3**	- Paragraph 4 of the ISO 27001 stresses the importance of identifying all relevant elements involved relevant to the project - In its Annex A, the ISO 27001 lists the control objectives that an ISMS should achieve and the types of controls for each of the objectives
Present in the proyect					x	**5**	- The first step of the project was, using the Anex A of the ISO 27001, to identify all the areas of the company relevant to the project

5.1 Plan Scope Management

	1	2	3	4	5	Score	Comments
Present in ISO 27001				x		**4**	- The paragraph 6.1.2 of the ISO 27001 contains guidelines for how the scope of an ISMS should be elaborated
Present in the proyect					x	**5**	- The main objective of the project was to achieve the certification against the ISO 27001 and the completion of the documentation required for the certification was used to manage the scope

5.2 Collect Requirements

	1	2	3	4	5	Score	Comments
Present in ISO 27001			x			**3**	- Annex A of the ISO 27001 is a list, with brief definitions, of all the controls that an ISMS can have
Present in the proyect					x	**5**	- Exhaustive review of all ISO requirements - Consideration of the applicability of all the ISO requirements to the organization - Proposal of how the applicable ISO requirements where going to be met - Determination of which stakeholders should be consulted before defining the controls that should be implementedirements

5.3 Define Scope

	1	2	3	4	5	Score	Comments
Present in ISO 27001				x		**4**	- Paragraph 4.3 of the ISO 27001 states that an organization should determine the scope of its ISMS
Present in the proyect					x	**5**	- Several meetings were needed to determine the reach of the ISMS - The fifth version of the scope was finally validated and it contains what is going to be included in the ISMS offices, CDPs, software's, hardware's, external providers, etc…

5.4 Create WBS

	1	2	3	4	5	Score	Comments
Present in ISO 27001			x			**3**	- Although the ISO provides a detailed list of all the possible controls that an ISMS could incorporate, it does not go into more detail than to provide a brief description for each of them
Present in the proyect				x		**4**	- Identification of all the ISO 27001 requirement applicable to the project and in witch ISO document could be found. - Compilation of any company policy, document or manual that needed modification to include information security notions

6.1 Plan Schedule Management

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- ISO 27001 provides the requisites for the implementation of an ISMS but it has no regard towards controling the time required to do so
Present in the proyect			x			3	- Limited to setting certain dates in which the different tasks or deliverables were expected to be finished

6.2 Define Activities

	1	2	3	4	5	Score	Comments
Present in ISO 27001				x		4	- The ISO 27001 includes a template that suggests a set of measures to improve the information security but the details have to be tailored to each specific ISMS
Present in the proyect					x	5	- Determination of every control to be implanted in the organization for each ISO requirement applicable for the ISMS - Detailed descriptions of each activity and control to be implemented

6.3 Sequence Activities

	1	2	3	4	5	Score	Comments
Present in ISO 27001		x				2	- The ISO 27001 presents the set of controls that a good ISMS should have in a format that can be followed to sequence the activities
Present in the proyect			x			3	- Most of the project activities were listed in the ISO template and were sequenced following the order set in it - Other activities, mostly related with requisites related to the integration of the ISMS in the company policies, were introduced in the sequence taking into account which activities had to be completed beforehand

6.4 Estimate Activity Durations

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- The ISO 27001 pays no attention to each activity duration, it only presents the complete spectrum of controls that an ISMS could have
Present in the proyect	x					1	- Rather than estimating an approximate duration for each of the activities the project team was informed of the dates the project deliverables were expected to be ready - Project team members were expected to ask for help if they estimated that they were not going to meet any particular deliverable date

6.5 Develop Schedule

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- The ISO 27001 does not provide guidance to develop an schedule to implement an ISMS
Present in the proyect				x		4	- Based on knowledge acquired in previous projects and considering past performances of the members of the project team a Gant diagram was developed

7.1 Plan Cost Management

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- The ISO 27001 does not contemplate how to manage, estimate or control the costs that the implementation of an ISMS could bring to an organization
Present in the proyect	x					1	- Once the management of the organization set the goal of certifying the company against the ISO 27001 there was little concern towards the cost that the project would represent and, in consequence, a cost management plan was not formulated

7.2 Estimate Costs

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- The ISO 27001 does not contemplate how to manage, estimate or control the costs that the implementation of an ISMS could bring to an organization
Present in the proyect		x				2	- Other that asking for a budget estimation from the consultancy agency there was no calculation of the cost that the time dedicated by the members of the organization would suppose

7.3 Determine Budget

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- The ISO 27001 does not contemplate how to manage, estimate or control the costs that the implementation of an ISMS could bring to an organization
Present in the proyect	x					1	- The organization did not set a particular budget for the project. Simply put, the certification against the ISO 27001 was considered as a requirement for the company and, as long as it could be achieved by mainly using the staff already in the IT department, there was little consideration to the costs

8.1 Plan Quality Management

	1	2	3	4	5	Score	Comments
Present in ISO 27001				x		4	- Section 9 of the ISO 27001 provides guidelines to establish a quality control system for an ISMS
Present in the proyect				x		4	- The certification against the ISO 27001 was the main objective of the project, therefore the planification of the quality management consisted in tailoring the recommendations of the standard to the particularities of the organization

9.1 Plan Resource Management

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- The ISO 27001 does not contemplate how to manage the resources required to implement or certificate an ISMS
Present in the proyect		x				2	- There was not a specific planification for the resource management of this particular project. The main resources were the team members, that were from the IT department and their management fell naturally upon the head of the department and project manager

9.2 Estimate Activity Resources

	1	2	3	4	5	Score	Comments
Present in ISO 27001		x				2	- The ISO 27001 merely notes that the organization should determine and supply the necessary resources for the implementation, control and maintenance of an ISMS. But does not go into specifics to which those resources may be
Present in the proyect			x			3	- The members of the IT department responsible for the completion of this project, were aware of its importance but there was not a formal estimation of the resources required to carry on each activity - Nonetheless, if at any time a member of the team could not comply in time, additional resources would have been assigned upon request

10.1 Plan Communications Management

	1	2	3	4	5	Score	Comments
Present in ISO 27001		x				2	- In its section 7.4, the ISO 27001 makes note of how important it is to communicate the requirements of the ISMS to any member of the organization that may have any impact on them - This is regarded as a requirement of an ISMS, an so it constitutes an activity that the project team had to deliver. What the ISO 27001 does not contemplate is how to manage communication to ensure the success of the project
Present in the proyect				x		4	- Communications between team members were conducted as they were already accustomed and using the same communication channels - When needed, any communication or notifications with other stakeholders from within the company were conducted using the preexisting channels - There had to be special consideration for the communication with the consulting company was required

11.1 Plan Risk Management

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- Although the ISO 27001 extensively covers the subject of risk management for information security and the maintenance of an ISMS, it does not consider what risks may impact its implementation or how to manage them
Present in the proyect	x					1	- Because of the nature of the ISO 27001 many of the project activities involved risk management (in relation with IS), but there has been no formal treatment of the risks that the project faced in any terms similar to what the PMBOK presents

11.2 Identify Risks

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- The ISO 27001 greatly emphasizes the importance of identifying possible information security risks as well as their sources but, it does not consider any risk (unrelated to IS) that may threaten the implementation project
Present in the proyect	x					1	- As in the previous item, the project performed risk identification as part of the activities required to implement and then certificate the ISMS, but no resources were allocated to the identification and documentation of individual project risks or their possible sources.

11.3 Perfform Qualitative Risk Analysis

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- The ISO 27001 in its paragraph 6.1.2 mentions the importance of systematically evaluating risks in order to prioritize them, but again, this exclusively refers to risks related to the information security
Present in the proyect	x					1	- As there was no formal identification of the risks that the project may encounter there was no prioritization either

11.4 Perform Quantitative Risk Analysis

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- The ISO 27001 in its paragraph 6.1.2 mentions the importance of systematically evaluating risks in order to prioritize them, but again, this exclusively refers to risks related to the information security
Present in the proyect	x					1	- As there was no formal identification of the risks that the project may encounter there was no prioritization either

11.5 Plan Risk Responses

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- As in the previous cases, the ISO 27001 only contains guidelines for the planification of responses for information security risks
Present in the proyect	x					1	- Again, many of the project activities consisted in developing responses to the identified information security risks but there was no formal consideration for the risks that the project may face and so, there was no responses planned in advance

12.1 Plan Procurement Management

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					**1**	- There is no mention in the ISO 27001 about how the purchase of goods or services that an ISMS may require should be managed
Present in the proyect		x				**2**	- The project manager did not consider the planification of procurement management of great importance to this particular project, due to its particularities and the fact that the company already has a department that manages the purchase of goods and services that the organization may require

12.2 Plan Stakeholder Engagement

	1	2	3	4	5	Score	Comments
Present in ISO 27001			x			**3**	- In its paragraph 7.3 the ISO 27001 mentions the importance of keeping everyone, whose actions may impact the information security, involved with the ISMS implementation or maintenance
Present in the proyect			x			**3**	- The stakeholder engagement plan merely contemplated informing each of the identified information security risk owners, notifying them about their "new" official responsibilities, and about any changes required from them to mitigate a particular risk

Executing Process Group

4.3 Direct and Manage Project Work

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					**1**	- The ISO 27001 does not consider how to improve the efficiency of the process or certification of an ISMS
Present in the proyect				x		**4**	- Short and highly structured meetings specially in the first stages of the project to ensure that every team member understood the task ahead. - Deliverables were set along the project schedulle to assess the progression of the project

4.4 Manage Project Knowledge

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					**1**	- Proper project knowledge management is not contemplated in the ISO 27001
Present in the proyect			x			**3**	- The organization has not a system in place to share "explicit" knowledge during the execution of past projects - Tacit knowledge management does not have a system in place either. In this particular project was limited to the past experiences of the project team members and, because of the relative seniority of the team members within the organization it proved sufficient

8.2 Manage Quality

	1	2	3	4	5	Score	Comments
Present in ISO 27001			x			**3**	- Requires an external audit to be certifiable
Present in the proyect				x		**4**	- Consisted in the evaluation of the different deliverables both by the hired consultants and the project management (independently). The results were put in common and corrections were implemented when needed

9.3 Acquire Resources

	1	2	3	4	5	Score	Comments
Present in ISO 27001			x			**3**	- The ISO 27001 acknowledges the importance of dedicating the appropriate resources for the implementation and maintenance of the ISMS
Present in the proyect				x		**4**	- A consulting agency was hired to provide support throughout the project - Any software or hardware deemed required to obtain the ISO certification was channeled through the company's usual purchase procedures

9.4 Develop Team

	1	2	3	4	5	Score	Comments
Present in ISO 27001					x	**5**	- In its paragraph 7.2 the ISO 27001 stresses the importance of ensuring that any member of the organization that may impact the ISMS has the required competences and, if needed, to provide training so they can develop them
Present in the proyect					x	**5**	- The project team was integrated by members of the IT department that were highly educated. In addition, at the beginning of the project they were provided with training so they could familiarize themselves with the ISO 27001 and its requirements

9.5 Manage Team

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					**1**	- The ISO 27001 does not cover the management of the team responsible for the implementation of the ISMS
Present in the proyect			x			**3**	- After the assignment of responsibilities to members of the IT department the control of the team management was limited to the provision of feedback upon request or on project deliverables - All the team members where already part of the staff and, when the project was launched, they began to work on their assignments as usuall

10.2 Manage Communications

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- Although the ISO 27001 mentions communication in its section 7.4 it is only in terms of mitigating the information security risks
Present in the proyect				x		4	- There was no specific action taken to manage communication amongst team members, it was not considered necessary because they were already members of the same department - The deliverables and any other document relevant for the project, were used an standardized format and were electronically archived in a private server so they were available for all the team - Communication with the consultants was managed via regular meetings and the exchange of information using shared digital storage

11.6 Implement Risk Responses

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- Although the ISO 27001 extensively covers the subject of risk management for information security and the maintenance of an ISMS, it does not consider what risks may impact its implementation or how to manage them
Present in the proyect	x					1	- Because of the nature of the ISO 27001 many of the project activities involved risk management (in relation with IS), but there has been no formal treatment of the risks that the project faced in any terms similar to what the PMBOK presents

12.2 Conduct Procurements

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- There is no mention about how procurements should be conducted in the ISO 27001
Present in the proyect			x			3	- Procurements were managed using the preexisting procedures within the organization

13.3 Manage Stakeholder Engagement

	1	2	3	4	5	Score	Comments
Present in ISO 27001		x				2	- Sections 7.3 and 7.4 of the ISO 27001 stablish the importance of keeping the stakeholders within the organization involved in the ISMS and aware of its requirements but does not contemplate how this involvement should be achieved
Present in the proyect			x			3	- Once the planned measures to comply with ISO 27001 were notified there was some feedback from certain stakeholders and, although in a few cases they translated in slight modifications, the stakeholder engagement was manly unidirectional

Monitoring and Controlling Process Group

4.5 Monitor and Control Project Work

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- ISO 27001, in its section 9, underlines the importance of having a complete system of monitorization, analysis and control of the ISMS but, similarly to what happened with risk management, this refers to the performance of the ISMS itself and not to the performance of the implementation project itself
Present in the proyect			x			3	- Limited to the evaluation of project deliverables, which proved to be insufficient as there were some unforeseen delays, specially during the final stages of the project

4.6 Perform Integrated Change Control

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- ISO 27001 does not include guidelines for how to perform changes in the implementation or certification of an ISMS, when mentioned changes in as ISMS are considered part of the maintenance it requires once it is already in place
Present in the proyect					x	5	- Due to the fact that normally they have to introduce changes in projects that they may not fully understand, the IT department, from which almost all team member were part of, already had an integrated change control system in place and ready to be used in this project

5.5 Validate Scope

	1	2	3	4	5	Score	Comments
Present in ISO 27001				x		4	- To be certifiable against the ISO 27001 an ISMS has to undergo an independent external audit, by a certified auditor, to validate its compliance with the requirement set in the standard
Present in the proyect					x	5	- Along the project duration there were a set of deliverables aimed to confirm the completion of the different project activities. - Before considering the project finished a full internal audit, executed by an external firm, was scheduled to corroborate that everything included in the scope was implemented and operational within the organization - Once the changes suggested by the first audit were introduced, the ISMS underwent the external audit and obtained the certification against the ISO 27001 standard

5.6 Control Scope

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- The references about controlling the scope found in the ISO 27001, specifically in its section 10, refer to the ISMS in itself and are more oriented to its maintenance once it is implemented in an organization
Present in the proyect				x		4	- The scope was controlled as part of the integrated change control process, that as mentioned was already in place. When needed, this helped to redefine the reach of the ISMS being implemented and so, achieve a better compliance with the standard and, ultimately, its certification against the ISO 27001

6.6 Control Schedule

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- The ISO 27001 does not provide guidance to control the implementation schedule of an ISMS
Present in the proyect			x			3	- Although present, the schedule controls proved to be a bit scarce and concentrated toward the end of the timeline in the form of deliverables - There were some unexpected delays due to the lack controls during the early-mid stages of the project

7.4 Control Costs

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- The ISO 27001 does not contemplate how to manage, estimate or control the costs that the implementation of an ISMS could bring to an organization
Present in the proyect		x				2	- There was little to no control of the costs in terms of hours dedicated by the project team to this project - After accepting the final offers for the consultancy and audit services the preexisting controls of the company entered in place to assure that there was no deviation from the agreed upon costs

8.3 Control Quality

	1	2	3	4	5	Score	Comments
Present in ISO 27001			x			3	- Requires an external audit to be certifiable
Present in the proyect				x		4	- Once implemented, the ISMS underwent an independent audit to ensure its readiness to face the final audit to be certified against the ISO 27001

9.6 Control Resources

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- The ISO 27001 does not consider how to control the appropriate use of the resources assigned to the implementation of an ISMS
Present in the proyect		x				2	- This particular project was not heavily reliant of physical resources. Therefore, there was not a resource control system in place

10.3 Monitor Communications

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- The ISO 27001 does not include communication monitorization
Present in the proyect	x					1	- The effects of the communications were not measured during the project

11.7 Monitor Risks

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- Although the ISO 27001 extensively covers the subject of risk management and monitorization for information security and the maintenance of an ISMS, it does not consider what risks may impact its implementation or how to manage them
Present in the proyect	x					1	- Because of the nature of the ISO 27001 many of the project activities involved creating system for risk monitorization (in relation with IS), but there has been no formal treatment of the risks that the project faced in any terms similar to what the PMBOK presents

12.3 Control Procurements

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- ISO 27001 does not contemplate how to control the procurement of the resources needed to implement an ISMS
Present in the proyect		x				2	- There is not a formal system for managing relationships and monitoring the performance of suppliers that do not supply raw material for the production of refrigerated display cabinets - In this case, the project manager is indirectly responsible for evaluating the performance of the suppliers involved, and take it into consideration if future needs of this type of services may appear

13.4 Monitor Stakeholder Engagement

	1	2	3	4	5	Score	Comments
Present in ISO 27001	x					1	- There is no mention in the ISO 27001 to the modification of strategies to further improve the stakeholder engagement in the ISMS or its implementation
Present in the proyect	x					1	- There was no measurement of the level of stakeholder engagement during the project and so there was no attempts to improve it either