BJRS

BRAZILIAN JOURNAL
OF
RADIATION SCIENCES
10-01 (2022) 01-27

SBPR
Sociedade Brasileira de Proteção Radiológica

Development of an effectiveness evaluation model of the security management function of radiological facilities

Lima[a,b,c] A.R., Germano[c] T.P., Da Silva[a] F.C.A.

[a] *Institute of Radiation Protection and Dosimetry (IRD), Av. Salvador Allende, 3773 – Barra da Tijuca, Rio de Janeiro – RJ – Brazil*

[b] *Brazilian Nuclear Energy Commission (CNEN), Rua General Severiano, 90 – Botafogo, Rio de Janeiro – RJ – Brazil*

[c] *Brazilian Institute of Radiological Sciences (INBRARAD), Av. Das Américas, 19005, Torre 2, Sala 225 – Recreio dos Bandeirantes, Rio de Janeiro – RJ – Brazil*

alexandre.r.lima1313@gmail.com

ABSTRACT

A Physical Protection System (PPS) is based on the five basic security functions (deterrence, detection, delay, response, and security management), all of which are required to protect a radiological facility against malicious acts. Evaluating the performance of the PPS, including security procedures and their implementation, is a way to engage workers from different hierarchical levels, raise their awareness on the importance of security. This article presents a new effectiveness evaluation model of the PPS administrative structure through qualitative analysis, which is appropriate for the security management evaluation of low-consequence radiological facilities, to protect them against malicious acts. This model was developed in 5 stages to obtain a structured process for conducting the PPS administrative structure evaluation, based on the security management function, consisting of 11 topics and 89 qualitative questions to determine the Relative Robustness Index of this function. Model topics were classified with distinct relative weights based on their relevance to the PPS. For testing and validation of the model, 6 industrial radiological facilities classified in different security levels were selected. The results showed that the self-assessment model proposed in this article is viable, considering its simplicity, promptness, and applicability in identifying and analyzing the strengths and weaknesses of the PPS security management function. The new model made possible the effectiveness evaluation of the PPS globally and punctually, making it possible to identify which topics of security management are above, or below, the minimum required for the current security level.

Keywords: **physical protection system, radiological facility, nuclear security, security level, radioactive source.**

ISSN: 2319-0612
Accepted: 2022-01-20

1. INTRODUCTION

The growing concern of the international community relating to the nuclear security of radioactive sources and associated facilities after September 11th, 2001 resulted in a strengthening, at world level, of the application of physical protection requirements for radioactive sources, associated facilities and associated activities through the adoption of new parameters and methodologies for the design and implementation of physical protection measures and systems [1].

The risk that radioactive sources could be used in terrorist acts is regarded as a serious threat to international peace and security [2].

There are currently in Brazil around 2,500 radiological facilities in operation, with approximately 500 Category 1 and 2 radioactive sources, according to IAEA (International Atomic Energy Agency) Categorization [3].

The National Nuclear Energy Commission (CNEN - in the Portuguese acronym) based on the comparative study of Lima *et al.*, and following the world trend, elaborated and published a specific regulation for the physical protection of radioactive sources, which provides for the principles and requirements on the subject, among which the requirement of the Physical Protection System (PPS) design by the licensee [4,5].

The PPS is based on the five basic security functions (deterrence, detection, delay, response, and security management), all of which are required to protect a radiological facility against malicious acts [6,7].

The design of the PPS is based on the fundamental "Graded Approach" principle, to achieve the objectives, goals, and sub-goals according to the applicable facility's IAEA Security Level A, B, or C [6].

Assigning the appropriate security level is about balancing risks with costs. Assigning a too high security level will require an unjustified expenditure on security resources given the risk, on the contrary, assigning a too low security level will expose the facility an excessive security risk [8].

The security management function addresses the establishment and implementation of policies, plans and procedures for the security of radioactive sources, as well as the deployment of the necessary resources for the effective operation of the other basic PPS security functions. Security management includes measures for access control, trustworthiness verification, information

protection, preparation of a security plan, training and qualification of personnel, accounting, inventory, and event reporting, among other measures that complement and allow the effective operation of the PPS [6].

The objectives of security management are to ensure an effective and sustainable PPS that meets regulatory requirements, including the provision of administrative measures of physical protection, integration of people, procedures, and equipment, and instill and promote a strong security culture [9].

Effective PPS is critical for business success. Evaluating the performance of PPS, including the security procedures and their implementation, is a way to engage with staff, raise their awareness on the importance of security, explain the benefit of good security, and finally ensure their engagement in security issues [10].

Research efforts have been carried out to evaluate and develop the PPS effectiveness, with the development of models, tools, and technologies for assessment. [11-13]

The PPS effectiveness evaluation models use quantitative or qualitative analysis. The PPS that are designed to protect high-value critical assets generally require a quantitative analysis. The PPS protecting lower-value assets may be analyzed using less rigorous qualitative analysis. [7]

The quantitative analysis uses the numerical estimation of PPS elements to assess its effectiveness against threats, where testing data is available, either from performance tests run on the PPS or from tests run in the laboratory [7]. Qualitative analysis, however, uses descriptors, rather than a numerical value, which is based on expert estimates and, therefore, it is necessary to rely on the competence and experience of the creators of the standards that use this analysis during the evaluation of PPS elements. [12]

Therefore, the quantitative analysis is often used in nuclear power plants (NPP) and other critical facilities to evaluate the PPS effectiveness, however, such evaluation models are complex, as they require tools and computer simulations. For smaller facilities compared to NPP, like radiological facilities, the effort and cost to perform a complex analysis is not feasible [13].

This article presents a new effectiveness evaluation model of the PPS administrative structure, Physical Protection System Effectiveness Evaluation Model (MAESP - in the Portuguese acronym), through qualitative analysis, which is appropriate for the security management evaluation of

radiological facilities, including medical and industrial facilities, to protect them against malicious acts.

2. BASES FOR DEVELOPING THE EVALUATION MODEL

This version of the Physical Protection System Effectiveness Evaluation Model (MAESP), for evaluating the administrative structure of the Physical Protection System (PPS), is based on the fundamental principle of graded approach.

It is a model for evaluating, which uses a qualitative analysis to assess the administrative measures inherent to the security management function, according to the security level adopted by the radiological facility.

For the development of MAESP, important premises and conditions for the creation of the evaluation model were considered:

- MAESP is focused on evaluating the effectiveness of the PPS administrative structure through the security management function. The other basic security functions, which make up a PPS physical structure, should be particularly evaluated for their effectiveness.
- The "Access Control" topic, which belongs to the security management function, was not considered in this model, as it is not possible to measure this topic as an administrative measure of physical protection, as it belongs to the physical structure of the PPS;
- The evaluation model was adapted with the inclusion of other topics, in addition to existing IAEA topics [6], such as "Security Culture", as it is a fundamental principle, in addition to the "Budget and Resource Planning" and "Maintenance Program", as they are important for the PPS sustainability, according to WINS [14];
- To grade the combined administrative measures in the PPS, the term Relative Robustness Index (RRI_1) was created, which considers all topics of the security management function with their relative weights (Rw);
- To measure the minimum robustness required for each security level, the term Required Robustness Index (RRI_2) was also created in MAESP, to indicate the robustness to be achieved by the security management function of the PPS, considering the graded approach principle.

3. METHODOLOGY

This version of the model was developed in 5 stages to obtain a structured process for conducting the PPS administrative structure evaluation, applied in radiological facilities (Figure 1).

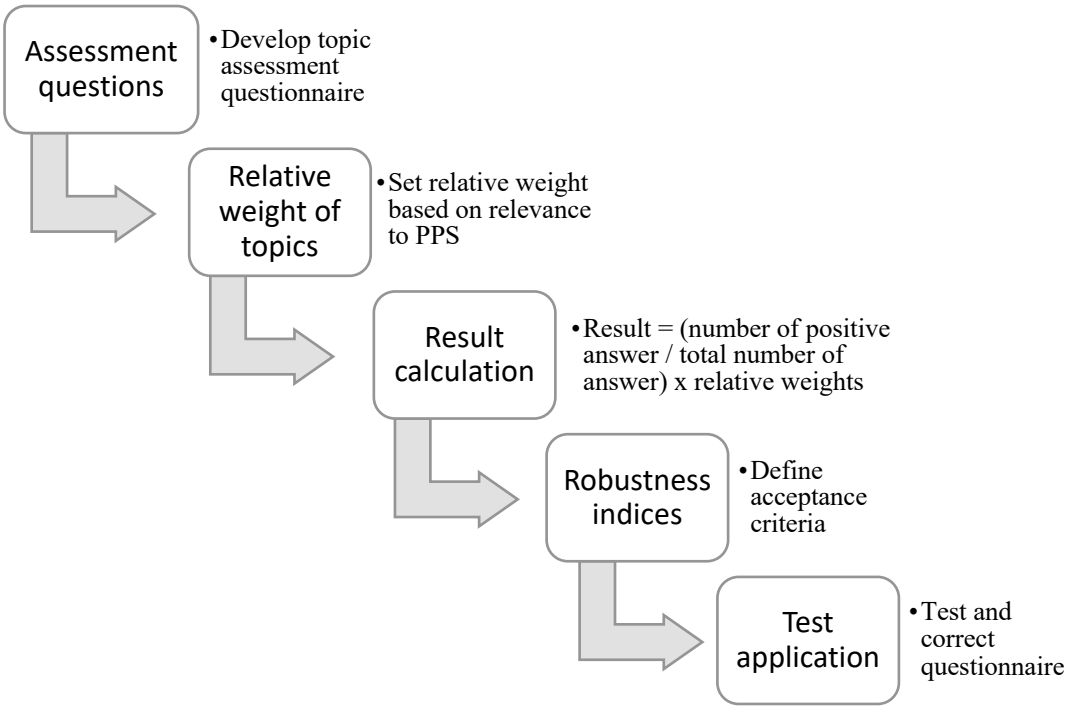

Figure 1: *Five stages to model design*

3.1 Stage 1: Development of the effectiveness assessment questionnaire by topic

At this stage, a self-assessment questionnaire was developed to assess the administrative structure of PPS, based on the security management function, consisting of 11 topics and 89 qualitative questions, based on IAEA [6] and WINS [14] guides, to determine the Relative Robustness Index (RRI_1) of this function. Figure 2 presents the topics, as well as their identification acronym in MAESP.

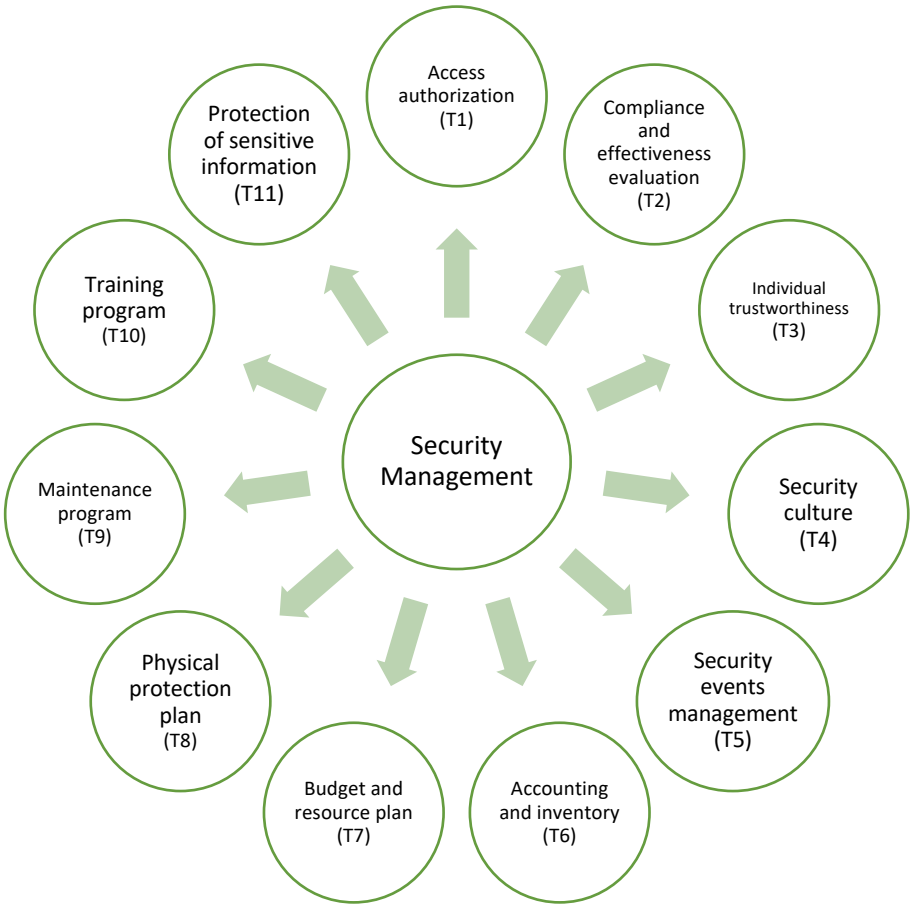

Figure 2: *Topics inherent in the self-assessment questionnaire*

The questions cover all topics to assess the adherence of administrative measures relating to the security management function in the radiological facility PPS. The number of questions per topic is different from each other, as each topic has its dimension and scope in terms of administrative measures for the system.

Five (05) qualitative questions were developed to assess the topic of Access Authorization, which matters for granting permission to access the radioactive source and/or access to sensitive information of the facility. For the topic of Compliance and Effectiveness Evaluation, which verifies the facility's compliance with physical protection regulatory requirements and effectiveness evaluation of the PPS, seven (07) questions related to the subject were prepared. The topic of Individual Trustworthiness, which provides the background check of an individual, who has permission to access the radioactive source and sensitive information, presents a set of ten (10) questions.

The topic of Security Culture presents fifteen (15) qualitative questions to assess the beliefs, values, behavior and attitudes of senior management, managers, and the workforce, encouraging awareness among employees about the role they play in physical protection of their organization.

The topic of Security Event Management, which encompasses a contingency plan with measures implemented for a series of potential security events, presents ten (10) questions on the topic. For the topic of Accounting and Inventory, which aims to detect the loss of the radioactive source through periodic checks, five (05) questions were raised.

Four (04) questions were developed to assess the topic of Budget and Resource Plan, which covers the human and funding resources to keep the PPS functional, efficient, and sustainable, from the purchase of the radioactive source to the final disposal.

The topic of Physical Protection Plan, with the design and operation of the PPS, presents seven (07) questions related to the topic.

The Maintenance Program and Training Program topics have nine (09) and eight (08) qualitative questions, respectively, to assess the adherence to both programs.

Finally, nine (09) questions were developed related to the topic of Sensitive Information Protection, with information such as guidelines and measures to protect information from unauthorized disclosure that could compromise the physical protection of the facility.

3.2 Stage 2: Definition of relative weight by topic

The determination of the relative weights was based on the authors' experience and judgment, considering the characteristics of the topic, and how relevant it is to the security management function of the PPS.

The 11 topics of the MAESP were classified with distinct relative weights, represented by a decimal number, with the sum of the weights equal to 1. Figure 3 shows the relative weights, represented by the acronym Rw, assigned to the topics of the security management function.

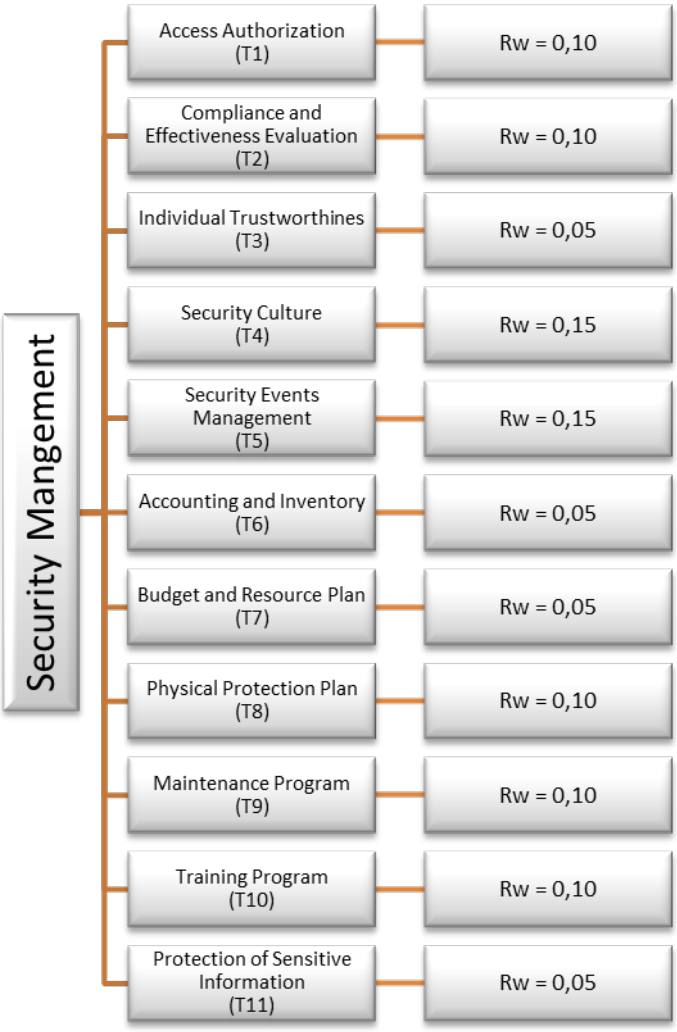

Figure 3: *Security management topics with relative weights*

The topics of Security Culture and Security Event Management received greater relative weight due to their greater relevance to the PPS, followed by the topics of Compliance and Effectiveness Evaluation, Physical Protection Plan, Maintenance and Training Programs. The remaining topics received a lower relative weight, classified with the same level of relevance in the MAESP.

The definition of the relative weights of each topic was established by the authors. However, these weights may be redefined by the evaluator, provided that the change is based on other sources of knowledge and bibliographies, demonstrating that the topic has greater or lesser relevance for the PPS. Furthermore, new topics can be inserted in MAESP, and their relative weight must be defined, following the same reasoning as above.

3.3 Stage 3: Description of parameters for calculating the relative robustness index

Since the questions pertaining to each topic have been developed based on international guidelines and recommendations on the radiological security, there is a need to properly analyze the answers to these questions. A simple, agile, and objective analysis methodology (adapted from KANG, Y [15]) that can be useful in evaluating the administrative structure of the PPS is suggested. A simple way to assess the answers, pertaining to certain topics of the security management function, is the calculation through the relative weights and the number of positive answers, that is, dichotomous questions that direct only two answers of bipolar character, of the yes/no type. This can show the global and partial results of security management topics.

The partial result of each topic is obtained by multiplying the rate of positive responses and relative weight, the partial result being represented by the acronym "PR_T", where "T" is the number referring to the topic assessed (Figure 2), according to equation (1):

$$PR_T = \frac{NPA}{NQ} xRw \tag{1}$$

where NPA is the number of positive answers for each topic, NQ is the number of questions for each topic, and Rw is the relative weight (Figure 3).

The global result is obtained through the sum of the partial results (PR_T), being adopted as the Relative Robustness Index (RRI_1) for the security management function, according to equation (2):

$$RRI_1 = \sum_{T=1}^{n} \frac{NPA_T}{NQ_T} xRw_T = \sum_{T=1}^{n} PR_T \tag{2}$$

3.4 Stage 4: Definition of required robustness index and acceptance criteria

The calculated RRI_1 should be correlated with the Required Robustness Index (RRI_2) acceptability ranges available in Table 1, which presents the acceptance criteria of “satisfactory” and “insufficient” based on the security level of the facility.

Table 1: Acceptance criteria based on the facility's security level

Acceptability Range of Required Robustness Index (RRI_2)	**Security Level**		
	A	**B**	**C**
$RRI_2 < 0,4$	Insufficient	Insufficient	Insufficient
$0,4 \leq RRI_2 < 0,6$	Insufficient	Insufficient	Satisfactory
$0,6 \leq RRI_2 < 0,8$	Insufficient	Satisfactory	Satisfactory
$0,8 \leq RRI_2 \leq 1,0$	Satisfactory	Satisfactory	Satisfactory

If the RRI_1 obtains an insufficient result ($RRI_1 < RRI_2$), the evaluator must individually identify the topics with results lower than the minimum required robustness index, with the objective of strengthening them punctually, and consequently, increasing the referring RRI_1 the security management function of the PPS, taking additional physical protection measures on these deficient topics.

After analyzing the RRI_1, MAESP presents a radar chart to allow a second analysis of the results, by topic, with the positive answer percentages obtained in the 11 topics and the minimum required robustness indices (RRI_2) referring to the A, B, and C security levels, as shown in Figure 4.

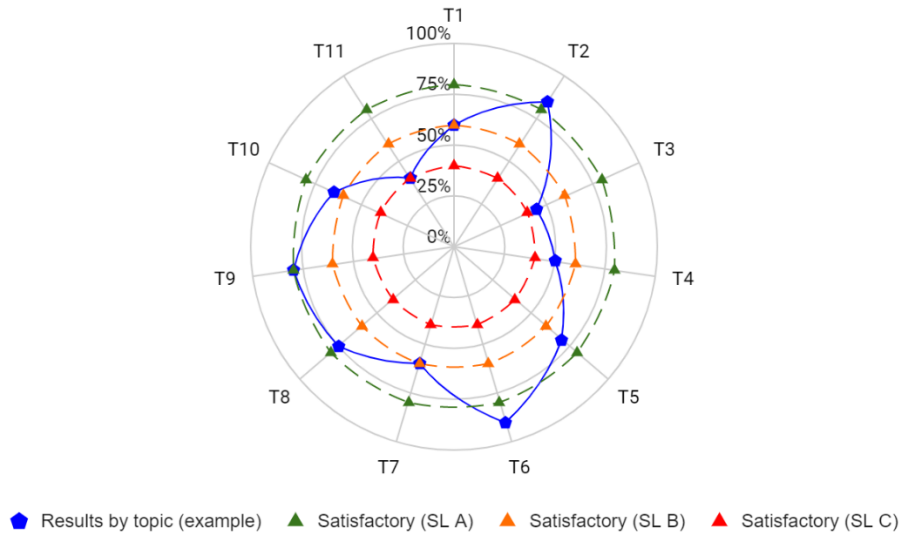

Figure 4: *Radar chart with examples of positive answre percentages by topic using A, B, and C security levels as a reference*

Adopting this type of graph, the “merit factor” is measured by the area inside the curve. The chart allows you to graphically visualize, in percentage terms, which topics have percentages below the minimum RRI_2, being subject to specific improvements.

If RRI_1 obtains a satisfactory result ($RRI_1 \geq RRI_2$), but the radar chart presents topics with results lower than the minimum RRI_2, there is a third acceptance criterion to be considered, called "conditioned", that is, the RRI_1 may present a satisfactory result, however, a specific topic can present results inferior to the acceptability range of RRI_2, its improvement being necessary to reach the minimum acceptability range, according to the security level.

Therefore, to obtain a fully satisfactory result, the PPS must reach the RRI_2 in both parameters, either in the calculated RRI_1 or in the percentage of positive answers, considering the acceptability interval, according to the security level.

3.5 Stage 5: MAESP test application for PPS evaluation

For the test application of the self-assessment questionnaire, six Brazilian industrial radiological facilities were selected, using sealed radioactive sources, classified in different security levels, being two industrial irradiation facilities (F1 and F2), two of industrial radiography (F3 and F4) and two of well logging (F5 and F6). In addition to obtaining the result of the effectiveness evaluation of the PPS administrative structure of these facilities, this phase made it possible to identify problems and/or doubts about the questionnaire, such as the proportion of "don't know" responses, difficult, ambiguous, and poorly formulated questions, the proportion of unanswered questions due to refusal, as well as the comments made by respondents on specific questions.

In this test, the questionnaires were sent to the facilities through *Google Forms*, and the answers were compiled in an electronic spreadsheet to analyze the calculated results.

3.6 Structured process for conducting the evaluation of the PPS administrative structure

MAESP uses the structured process identified in Figure 5, starting with the definition of the facility’s security level, followed by filling out the self-assessment questionnaire and analyzing the effectiveness of the RRI_1 and calculated percentages of positive answers, comparing the results with the RRI_2 for the security level previously defined.

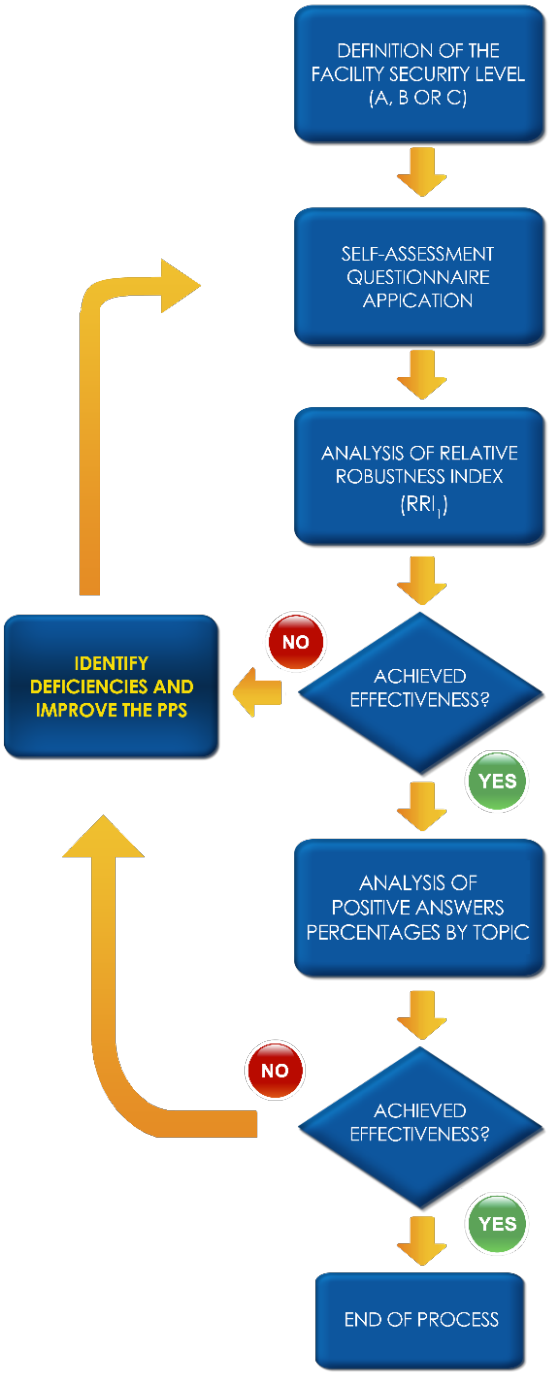

Figure 5: *Structured process for effectiveness evaluation of the PPS*

4. RESULTS AND DISCUSSION

This section presents the result of applying the MAESP, starting with the analysis of the questions formulation designed to identify inconsistencies in the questionnaire, followed by the analysis of the calculated results obtained from the answers from the radiological facilities, following the sequence presented in the structured process for effectiveness evaluation of the PPS (Figure 5).

4.1 Analysis of the developed questions formulation

Part of the respondents' comments at the end of some types, justifying the answers marked as "no" and "I don't know". Basically, some answers marked "no", with comments, reported as legal limitations for implementing administrative measures related to the topic of individual trust. The analysis of answers marked as "I don't know", which received comments from respondents, showed that some physical protection measures, which can be implemented in the administrative structure of the PPS, were not understood. Based on the comments, only punctual text modifications were implemented in the self-assessment questionnaire.

4.2 Analysis of self-questionnaire results

Following the sequence of the structured process (Figure 5), based on the answers obtained, each facility presented the results, as shown in Table 2.

Table 2: Self-assessment questionnaire results

Topic Partial Results and Relative Robustness Index	Radiological facilities (F)					
	F1	**F2***	**F3**	**F4**	**F5**	**F6**
PR_1	0,08	-	0,10	0,10	0,10	0,10
PR_2	0,04	-	0,07	0,04	0,07	0,06
PR_3	0,02	-	0,03	0,03	0,04	0,04
PR_4	0,13	-	0,12	0,08	0,15	0,12
PR_5	0,14	-	0,14	0,12	0,14	0,06
PR_6	0,05	-	0,05	0,05	0,05	0,04
PR_7	0,04	-	0,04	0,01	0,05	0,03
PR_8	0,10	-	0,10	0,10	0,07	0,00
PR_9	0,01	-	0,06	0,01	0,06	0,00
PR_{10}	0,08	-	0,08	0,04	0,10	0,06
PR_{11}	0,02	-	0,04	0,05	0,04	0,05
RRI_1	**0,70**	**-**	**0,81**	**0,63**	**0,86**	**0,55**

*Radiological facility F2 did not respond to the self-assessment questionnaire within the predetermined period.

Answers marked as “I don't know” during the test were considered negative for the purpose of calculating the results.

F1 facility, classified in security level A (SL A), presented an RRI_1 slightly lower than the minimum RRI_2 of 0.8, obtaining an insufficient result according to the criteria presented in Table 1.

The facilities of SL B, designated in this article as F3 and F4, presented an RRI_1 higher than the minimum RRI_2 of 0.6, reaching a satisfactory result according to the criterion in Table 1, where it is worth noting that the RRI_1 of the F3 facility was widely presented higher than RRI_2, considering SL B.

F5 and F6 facilities, with SL C, also presented an RRI_1 higher than the minimum RRI_2 of 0.4, reaching a satisfactory result according to the criteria in Table 1. Nevertheless, F5 facility had the highest RRI_1 among the evaluated facilities, being vastly superior to RRI_2 considering SL C.

Following the sequence of the structured PPS evaluation process (Figure 5), each topic was assessed individually, using the radar chart shown in Figure 6, where in this second analysis of the MAESP, the positive answer percentages obtained by topic of the F1 facility (blue pentagons) were compared to the minimum RRI_2 in percentage terms equivalent to SL A (dashed green line).

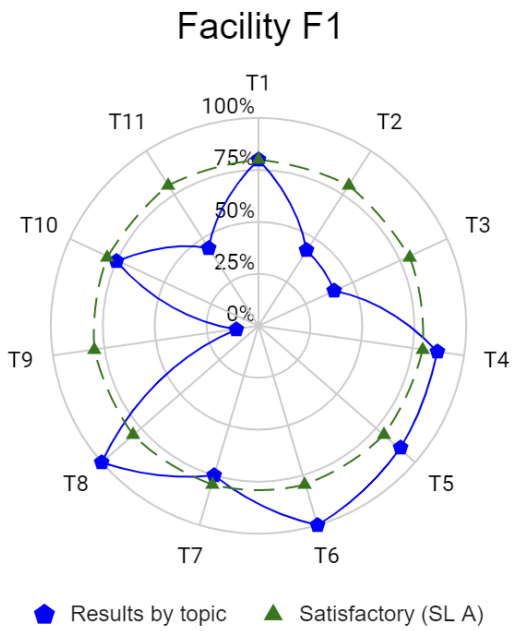

Figure 6: *Positive answer percentages by F1 facility topic based on SL A*

Analyzing the results, it was observed that the F1 facility presented 6 topics of the security management function with percentages of answers below the minimum RRI_2 of 80% (Table 1), requiring the adoption of additional physical protection measures in T2, T3, T7, T9, T10, and T11. T9 topic of the self-assessment questionnaire, for example, referring to the maintenance program (Figure 2), had an adherence of 10%, which means that only 1 out of the 10 questions (Appendix I) was positive, thus being the most deficient of the F1 facility.

The graph in Figure 7 shows the positive answers percentages by topic for F3 and F4 facilities (blue pentagons), considering the minimum RRI_2 equivalent to SL B (dashed orange line).

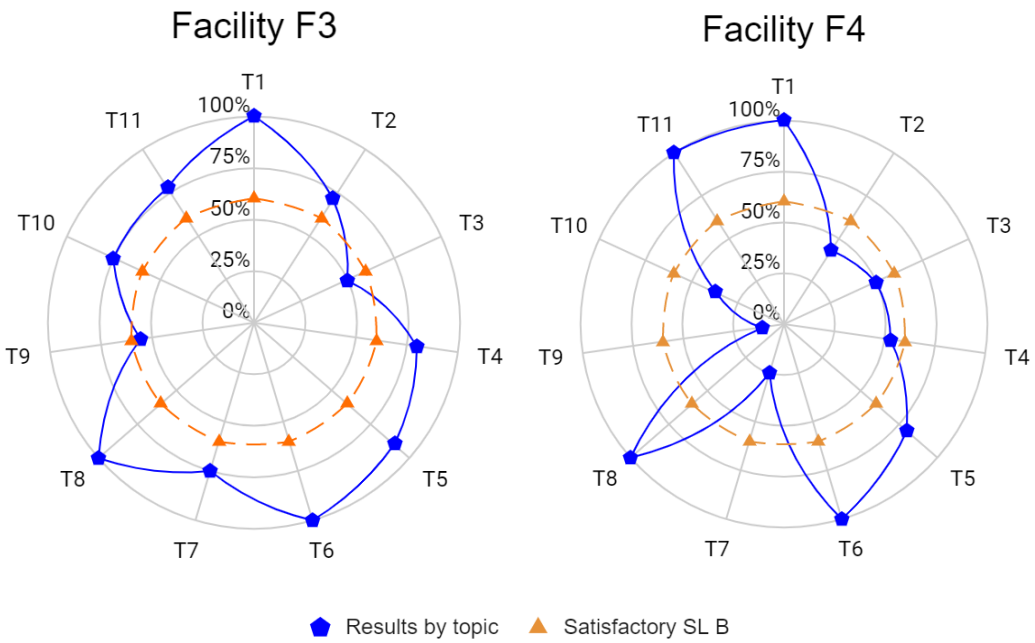

Figure 7: *Positive answer percentages by topic of F3 and F4 facilities based on SL B*

It was previously observed that, despite the RRI_1 of F3 facility having presented a satisfactory result, two topics presented positive answer percentage results of slightly lower than the minimum RRI_2 of 60% (Table 1), culminating in a result considered as conditioned. Therefore, it is necessary to implement specific improvements in the individual trustworthiness and maintenance program topics (T3 and T9), with the addition of at least one physical protection measure in each topic, to achieve the fully satisfactory result of the security management function of the PPS. F4 facility also presented a result considered as conditioned, however, a greater number of topics with percentage results below the minimum RRI_2 lower percentages of adherence to the questionnaire questions (Appendix I), and should implement improvements in topics T2, T3, T4, T7, T9 and T10, with additional physical protection measures to achieve the fully satisfactory result of the PPS security management function.

The graph in Figure 8 shows the positive answer percentages by topic for F5 and F6 facilities (blue pentagons), considering the minimum RRI_2 of SL C (dashed red line).

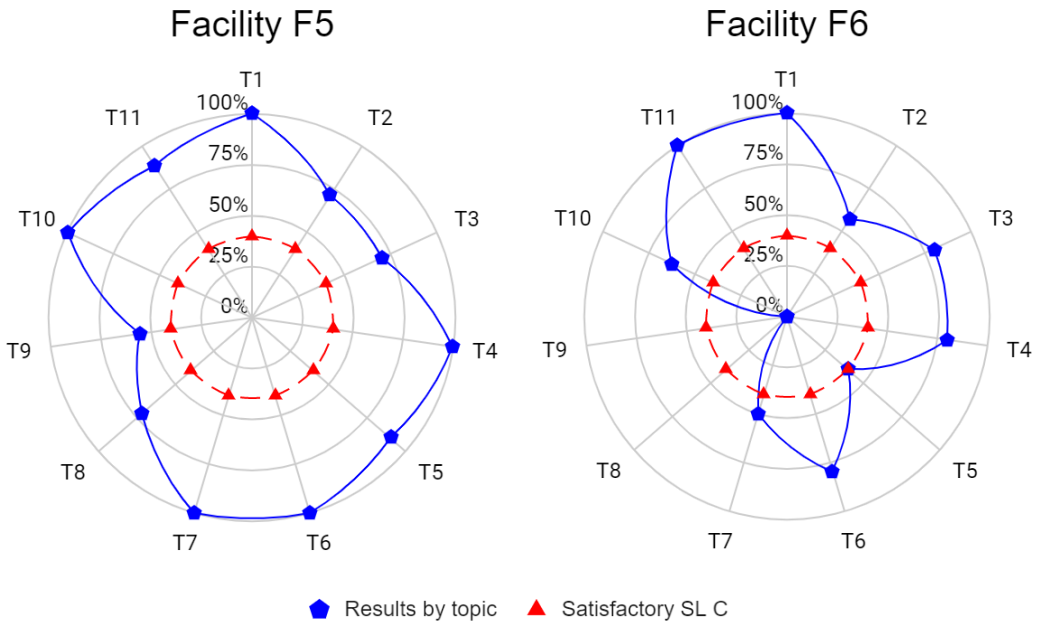

Figure 8: *Positive answer percentages by topic of F5 and F6 facilities based on SL C*

Analyzing the results obtained by F5 and F6 facilities, it was observed that F5 facility reached, in all commons, percentages of positive answers higher than the minimum RRI_2 of 40%, equivalent to SL C, being the PPS security management function of this facility being considered satisfactory, based on MAESP criteria. F6 facility also presents very positive results in most of the common ones, except in T9 of the self-assessment questionnaire, referring to the maintenance program (Figure 2), where no positive answer was obtained to the 10 existing questions (Appendix I), therefore it is the only flawed topic of the F6 facility's PPS security management function to be improved with the addition of physical protection.

5. CONCLUSIONS

The Physical Protection System is composed of a physical structure capable of preventing radiological sabotage and/or unauthorized removal of a radioactive source present in the radiological facility, however, this system must be complemented by an administrative structure, conducted by the security management function, which establishes the general policies, plans and procedures for

the implementation of physical protection, integration of people, procedures and equipment, and promoting a strong security culture at the facility, in order to guarantee the effectiveness and sustainability of the PPS.

With the scarcity of practical models for effectiveness evaluation of PPS, the self-assessment model proposed in this article proved to be viable, considering its simplicity, timeliness, and applicability in identifying and analyzing the strengths and weaknesses of the PPS security management function of the radiological facility.

The new model allowed evaluating the effectiveness of the PPS in a global and punctual way, giving the evaluator the possibility to identify which topics of security management are above, or below, the minimum necessary for the current security level, enabling the decision making to provide a balance of the facility's actual physical protection measures, using as a basis the measures listed in Appendix I.

MAESP was created based on a qualitative analysis methodology, making it much more understandable and agile in the assessment of the PPS administrative structure of a radiological facility, being very useful for use by professionals, auditors and consultants who work in the security sector, including as a self-assessment tool.

In MAESP, the evaluator can add new questions to existing topics, and add new topics to the evaluation model, if there is a credible basis for this, based on other sources of knowledge and bibliographies.

From this perspective of analysis, through the relative robustness indices (RRI_1), MAESP showed that the radiological facilities evaluated in this article obtained good results, however, in the analysis by topic, it was clear that the F1, F4, and F6 facilities did not present a tolerable leveling between the results of the physical security management function topics, showing that some are superior, and other topics that are largely inferior to the required robustness index (RRI_2), it being urgent the balance of physical protection measures in the PPS in these facilities.

It should be noted that the PPS administrative structure must be complemented by a physical structure, conducted by the other basic security functions (deterrence, detection, delay and response), endowed with elements such as fences, vaults, hardened buildings, hardened doors, cages, tie-downs, sensors and assessment devices, access control elements, communication devices, protective force

personnel, among other elements, and this PPS physical structure must be particularly evaluated for its effectiveness.

Based on the proposed model, the development of an effectiveness evaluated model for the PPS physical structure considering the other basic security functions is necessary as additional research.

REFERENCES

[1] LIMA A. R.; FILHO J. S. M.; MELLO L. A. **New brazilian regulation for security of radioactive sources**, In: International Conference on Nuclear Security: Commitments and Actions, IAEA, Austria, 2016.

[2] CNEN – Comissão Nacional de Energia Nuclear. **Sistema de instalações radiativas da CNEN – SIR**. CNEN, Brasil. Acessado em: 30/12/2021.

[3] IAEA – International Atomic Energy Agency. **Nuclear security systems and measures for the detection of nuclear and other radioactive material out of regulatory control**. **IAEA-NSS-21**, Implementing Guide, Austria, 2013

[4] LIMA, A.R., TAVARES, R.L.A., MONTEIRO FILHO, J.S., DA SILVA, F.C.A., **Panorama da segurança física de fontes radioativas no Brasil,** Brazilian Journal of Radiation Sciences, 06-02-B, 01-16, 2018

[5] CNEN, Comissão Nacional de Energia Nuclear, **Proteção física de fontes radioativas e instalações associadas**. **Norma CNEN-NN-2.06**, Resolução CNEN 254/2019. Available in: https://www.gov.br/cnen/pt-br/acesso-rapido/normas/grupo-2/grupo2_nrm206.pdf

[6] IAEA - International Atomic Energy Agency. **Security of radioactive material in use and storage and of associated facilities, IAEA-NSS-11-G Revision 1**, Implementing Guide, Austria, 2019.

[7] GARCIA, M. L. **The design and evaluation of physical protection systems**, Second Edition, Butterworth-Heinemann, Elsevier Science, USA, 2008.

[8] GARCIA, M. L. **Vulnerability assessment of physical protection systems**, First Edition, Butterworth-Heinemann, Elsevier Science, USA, 2006.

[9] IAEA - International Atomic Energy Agency. **Nuclear security recommendations on radioactive material and associated facilities, IAEA-NSS-14**, Recommendations, Austria, 2011.

[10] WINS - World Institute for Nuclear Security. **Methodology for assessing the effectiveness of security arrangements at gamma irradiation Facilities**, WINS Performance and Evaluation Series, Austria, 2021.

[11] EL WELY, C.; CHETAINE, A. **Analysis of physical protection system effectiveness of nuclear power plants based on performance approach,** Annals of Nuclear Energy 152 (2021) 107980

[12] LOVECEK, T.; VACULÍK, J.; KITTEL, L. **Qualitative approach to evaluation of critical infrastructure security systems**, European Journal of Security and Safety 1 (1) (2012) 1-11

[13] HOJNACKE, M. D.; CALLAHAN S. N.; SPARKS M. H.; BENTON JR, W. A.; MAY M. P.; MCDOWELL G. R.; PINCOCK M. R.; ROGERS J. A.; SANDOVAL J. S.; UECKER N. J. **Qualitative physical protection system security risk assessment methodology**, International Conference on Physical Protection of Nuclear Material and Nuclear Facilities. Vienna, 13-17 nov 2017. Austria, 2018. (IAEA/STI/PUB/1831; CD-2570).

[14] WINS - World Institute for Nuclear Security. **Radioactive source security management text-book**, Nuclear Security Management Certification Program, Austria, Standalone Module, 2019.

[15] KANG, Y.; CHONG, K. T. **Development of cyber security assessment methodology for the instrumentation & control systems in nuclear power plants**, Journal of the Korean Society for Industry-Academic Technology, Vol. 11, No. 9 pp. 3451-3457, 2010.

APPENDIX I

Topic	Self-assessment questions
Access Authorization (T1)	1. Is there a written access authorization policy? 2. Are there defined criteria, regarding reliability, trustworthiness, and training, for granting employee access authorization? 3. Are there defined criteria for excluding employee access authorization when they are fired or change roles? 4. Is there a visitor access control implemented? 5. Are visitors properly identified and accompanied during the visit to the facility's security areas?
Compliance and Effectiveness Evaluation (T2)	1. Is there an internal compliance assessment to periodically assess the effectiveness of PPS and identify possible deficiencies and opportunities for improvement in the facility? 2. Is the compliance assessment carried out by an organization or an independent auditor? 3. Are assessments carried out to verify that the team understands PPF, follows the procedures and uses the system properly and as intended? 4. Are assessments carried out to verify that the procedures produce the desired result and that the staff understands them? 5. Are assessments carried out to verify that the equipment works as intended and it is effective? 6. Are simulations and exercises carried out to assess the operationality and effectiveness of the PPS? 7. Are assessments of the PPF effectiveness carried out using any other analysis methodology, tool, or software?
Individual Trustworthiness	1. Is there a program to deal specifically with the insider threat, such as behavioral observation or others?

(T3)	2. Do employees believe an insider threat is credible and what appropriate mitigation measures should be taken? 3. Would employees report suspicious behavior by employees and contractors? 4. Are identity confirmations carried out prior to hiring the employee? 5. Are medical and psychological assessments carried out for hiring the employee? 6. Are background checks carried out on all employees with access to the radioactive source? 7. Are criminal background checks performed on all employees with access to the radioactive source? 8. Are toxicological tests performed on all employees with access to a radioactive source? 9. Is there a sanctioning process for personnel who do not comply with physical protection procedures? 10. Is there a written procedure with steps to be followed when there is a termination of the employment contract?
Security Culture (T4)	1. Does senior management believe the external threat to radioactive sources is credible? 2. Does senior management believe an insider threat is credible? 3. Does senior management believe that effective physical protection can manage and reduce risk? 4. Does senior management invest in an approach that integrates radiation protection and physical protection? 5. Does senior management demonstrate its commitment to physical protection through words and actions? 6. Does senior management treat physical protection features as a priority in the organization's business plan? 7. Does senior management have a written security policy?

	8. Do managers, on their own initiative, monitor the behavior of the workforce in general about physical protection? 9. Do managers provide good examples regarding the security culture? 10. Managers always consider employees' opinions on physical protection issues. 11. Do managers conduct periodic formal reviews to assess the effectiveness of physical protection instructions at work? 12. Are employees encouraged to share their physical protection concerns? 13. Are employees encouraged to resolve physical protection issues through group work. 14. Are employees regularly informed of physical protection issues on the premises? 15. Is there evidence of follow-up action when physical protection concerns are expressed by staff?
Security Events Management (T5)	1. Is there a contingency plan developed and approved by the regulatory body? 2. Is the contingency plan periodically reviewed to ensure it is current and always effective? 3. Does the facility periodically assess threats (external and internal) that may cause damage to radioactive sources and the facility? 4. Is there an armed response force at the facility or a memorandum of understanding (MoU) or similar security response agreement with outside organizations (e.g., police, security company)? 5. Are the responsibilities of all relevant employees and external organizations clearly defined in the contingency plan? 6. Are the response actions contained in the contingency plan periodically tested?

	7. Is there up-to-date technical information and color photographs of each equipment that contains a radioactive source in the facility files? 8. Are employees trained to prepare them to report or manage an event or incident involving a radioactive source at your facility? 9. Are response force-specific induction trainings conducted (e.g., facility familiarization, radiation protection, etc.)? 10. Are security events and incidents notified and reported immediately to the regulatory body?
Accounting and Inventory (T6)	1. Is there an established radioactive source inventory list that is kept up to date based on new acquisitions, transfers, and disposals? 2. Is periodic accounting of the quantity of existing radioactive sources carried out to confirm the presence of sources in the facility? 3. Is there a record of movement of the radioactive source, whether inside or outside the facility? 4. Are monthly radioactive source inventory checks carried out to assess the accuracy of the inventory record and movement records? 5. Are radioactive source and shielded container serial number checks carried out to confirm that the correct source belongs to that container?
Budget and Resource Plan (T7)	1. Is there a good management practice to maintain a minimum inventory of radioactive sources to meet the facility's needs? 2. Is there a fund saved to cover costs for disposing of the radioactive source when it is not in use? 3. Is there a specific budget for the maintenance program for physical protection devices? 4. Is there a specific budget for the physical protection training program?

Physical Protection Plan (T8)	1. Is there a physical protection plan (PPP) developed by the facility and approved by the regulatory body? 2. Is the PPP periodically reviewed to ensure it is up to date? 3. Are physical protection responsibilities clearly defined in the PPP? 4. Does the PPP describe in detail the physical protection system (PPS) existing in the facility? 5. Does the PPP present the records related to PPS? 6. Has the PPP been implemented and exercised with a view to its effectiveness and sustainability? 7. Have specific physical protection procedures, such as key control procedure, surveillance, access control, etc., been developed separately?
Maintenance Program (T9)	1. Is there a written inventory of all physical protection devices, including the purpose and function of each for PPS? 2. Are devices tested at the frequency recommended by the manufacturer? 3. Does the program identify the consequences and costs that could occur if each device fails? 4. Does the program identify the frequency and determine what are the acceptable failure rates for each device? 5. Does the program quantify the average time it would take to obtain replacement parts? 6. Does the program define what kind of features are available as replacement measures and how much time, money and effort would be required to get the device up and running again? 7. Does the program have a log of device failures, repairs, and lessons learned? 8. Does the maintenance program address the preventive actions to be performed on PPS devices?

	9. Does the maintenance program address the corrective actions to be taken on the PPS devices, to resume their operation as soon as possible? 10. Is there a written inventory of all physical protection devices, including the purpose and function of each for PPS?
Training Program (T10)	1. Is there a physical protection training program related to the skills required by physical protection staff and other facility personnel? 2. Are physical protection training provided to newly hired employees? 3. Are refresher trainings carried out regularly at pre-defined periods? 4. Are refresher training conducted after a security related event to prevent a recurrence? 5. Do employees assess their perception of their satisfaction in participating in the training? 6. Are employees assessed for retention of knowledge acquired in training? 7. Are employees evaluated to identify whether there has been a real improvement in their work routine after training? 8. Is there a security awareness training program for other employees at the facility?
Protection of Sensitive Information (T11)	1. Is information security part of the overall risk management strategy? 2. Has the organization identified and classified sensitive information? 3. Has the organization developed information security procedures that describe how sensitive information needs to be handled and protected? 4. Are physical protection plans and procedures available only to employees with proper access authorization? 5. Are physical protection procedures available only to employees who are responsible for specific physical protection actions?

	6. Is there any instrument (term, contract, etc.) that guarantees employees or third parties a commitment to maintain confidentiality before any access to sensitive information, with non-compliance subject to sanctions/ punishments, under the terms of the law? 7. Do information security procedures include actions to be taken in case of unauthorized disclosure? 8. Are employees and contractors who need access to sensitive information subject to background checks? 9. Did the team receive specific training or awareness sessions about the need for information security?