Exp- I- 3098

REPUBLICA DEL PERU

INSTITUTO PERUANO DE ENERGIA NUCLEAR

Resolución de Presidencia

N° 131-11-IPEN/PRES

Lima, 9 de Junio de 2011

VISTO: El Memorándum N°162-11-OTAN, del Director de la Oficina Técnica de la Autoridad Nacional.

CONSIDERANDO:

Que, el Organismo Internacional de Energía Atómica, OIEA, recomienda observar, medidas de seguridad física de las fuentes de radiación, mediante la adecuada legislación que permita una mejor y confiable seguridad física de las fuentes de radiación y nucleares, recomendaciones contenidas en el Código de Conducta Revisado sobre Seguridad Tecnológica y Física de las Fuentes Radiactivas: IAEA/CODEOC/2004, y que contribuyen a disminuir el riesgo que se produzcan atentados o actos maliciosos con estas fuentes;

Que, la seguridad radiológica y física es aplicable a todas las fuentes radiactivas que no se encuentren exentas del control regulador;

Que, de conformidad con lo establecido en el Reglamento de Seguridad Radiológica, aprobado por Decreto Supremo N° 009-97-EM, las fuentes radiactivas requieren ser protegidas de forma adecuada a fin de prevenir o reducir la posibilidad de uso malicioso contra las personas, población y medio ambiente;

Que, en aplicación de las facultades conferidas a la Autoridad Nacional en el ámbito de la energía nuclear mediante Ley N° 28028, Ley de Regulación del Uso de Fuentes de Radiación Ionizante y la Tercera de la Disposiciones Complementarias del Reglamento de la Ley, aprobado por Decreto Supremo N° 039-2008-EM, se expide la Norma Técnica cuya aplicación tiene alcance nacional;

De conformidad con el inciso b) de artículo 10° del Reglamento de Organización y Funciones, aprobado por Decreto Supremo N° 062-2005-EM;

Con el visto del Director de la Oficina Técnica de la Autoridad Nacional y de la Directora de Asesoría Jurídica;

SE RESUELVE:

Artículo Primero.- Aprobar la Norma Técnica "Requisitos de Seguridad Física de Fuentes Radiactivas", que consta de diecisiete (17) folios, la misma que debidamente rubricada forma parte de la presente Resolución.

Artículo Segundo.- La Norma Técnica que se aprueba con la presente Resolución, será publicada en la página Web de la Institución: http://www.ipen.gob.pe y en el Portal del Estado Peruano: http://www.peru.gob.pe.

REGISTRESE Y COMUNIQUESE

CARLOS BARREDA TAMAYO
Presidente
Instituto Peruano de Energía Nuclear

INDEX

0. INTRODUCTION

In accordance with the Radiological Safety Regulation, radioactive sources need to be adequately protected in order to prevent or reduce the possibility of malicious use against people.

1. OBJECTIVE

101. The standard describes the physical security requirements that must be applied to radioactive sources according to their level of risk.

2. REACH

201. The requirements of the standard are applicable to all radioactive sources that are not exempt from regulatory control.

3. DEFINITIONS

301. The definitions that apply to this standard are the following:

a) Activity: Measurement of the amount of radioactive material, defined by the expression:

$$A = \frac{dN}{dt}$$

where dN is the expected value of the number of spontaneous transformations that take place in the time interval dt. The unit of activity is the s^{-1} with the special name Becquerel (Bq).

b) Security Threat: Action or Condition that results or could result in an unauthorized removal of the source or a failure of the physical security system.

c) Authorization: either Registration, service authorization license granted to a natural or legal person to manage radioactive sources

d) LSA1: Low specific activity radioactive material, as defined in the Regulations for the Safe Transport of Radioactive Materials (http://www.iaea.org/publications/PDF/Pub1384s_web.pdf) in non-exempted quantities.

e) Radioactive package: Packaging with its radioactive content as it is presented to be transported.

f) Packaging: Set of components necessary to fully accommodate the radioactive content to be transported.

g) Radioactive source: Radiation source that contains radioactive material, whether it is in use, disused or as radioactive waste, which is not exempt from control.

h) Sealed radioactive source: Radioactive source where the radioactive material is sealed in a capsule or tightly bound and in solid form. This source can be fixed, mobile.

i) Human force: Any force exerted by a person, including the use of tools, but excluding energized tools.

j) Management: All administrative and operational activity involved in the manufacture, supply, receipt, possession, storage, use, transfer, import, export, transport, maintenance, recycling or final disposal of radioactive sources.

k) Radioactive material in non-special form: Material that is in a form such that it can be dispersed and is not sealed in any capsule.

l) Physical security measure: Engineering strategy or device that is implemented as an element of a physical security system.

m) Threat level: Indicator of the possibility that a perceived adversary obtains radioactive sources for illicit purposes. The threat levels are:

(i) high: high probability of unauthorized removal, theft or sabotage and where the existing level of deterrence and defense is inadequate

(ii) medium: medium possibility of unauthorized withdrawal, theft or sabotage and where the existing level of deterrence and defense are moderately adequate

(iii) low, very low or insignificant: little possibility of withdrawal, theft or sabotage and where the existing level of deterrence and defense are adequate

n) Security level: Level to which a radioactive source must be protected, according to its category and environmental factors.

o) OCSI: Object contaminated solid superficially in which:

(i) non-fixed contamination in the accessible area averaged over 300 cm2 does not exceed 4 Bq/cm2 for low toxicity beta, gamma and alpha emitters, or 0.4 Bq/cm 2 for the other alpha emitters,

(ii) fixed contamination on the accessible surface averaged over 300 cm 2 does not exceeds 4 x 10 4 Bq/cm 2 for low toxicity beta, gamma and alpha emitters, or 4 x 10 3 Bq/cm 2 for other alpha emitters (iii) fixed

plus non-fixed contamination on the inaccessible surface averaged over 300 cm 2 no exceeds 4 x 10 4 Bq/cm 2 for low toxicity beta, gamma and alpha emitters, or 4 x 10 3 Bq/cm 2 for the other alpha emitters

p) Adversary: Person who commits or carries out an illegal or criminal act.

q) Physical security plan: Plan that includes means and measures which is implemented to effectively minimize physical security risks relevant to Categories 1, 2 and 3. r) Radionuclide: Nuclide that undergoes

spontaneous transformation emission of ionizing radiation.

s) Physical security: Set of measures aimed at preventing unauthorized access or damage to radioactive sources, and the loss, theft or unauthorized transfer of these sources.

t) Radiological safety: Measures and means to control exposures as well as to prevent accidents and mitigate their consequences if they occur.

u) Physical security system: Combination of security measures described in a security plan that seek to achieve the physical security of a Category 1, 2 and 3 radioactive source.

v) Holder of the authorization: Natural or legal person that has a License or Current Services Authorization and is responsible for the radiological and physical safety of use during the management of radioactive sources

w) Intermodal transport: Transport of radioactive material by various routes such as land, sea, air

x) D-Value: This is the specific activity of radionuclides in a source that, if not under control, could cause severe deterministic effects in a variety of hypothetical exposure circumstances, including unshielded source and exposure from dispersion of the source material.

4. GENERAL REQUIREMENTS

401. The Holders of an authorization must apply physical security measures that prevent the theft, damage or unauthorized use of radioactive sources under their responsibility, through a physical security system that includes deterrence, detection, delay and response. before the attempt of a possible intrusion, attempted removal or damage of the sources.

402. The physical security measures applicable during the management of radioactive sources must not be detrimental to their physical security and radiological protection.

403. The holders of an authorization or senders of radioactive sources must designate a person responsible for physical security in the case of Category 1, 2 and 3 sources, or the transport of medium and high security level materials.

404. The transfer of radioactive sources must be carried out between natural or legal persons who have valid authorization and prior specific authorization from the Technical Office of the National Authority (NATO).

405. The holders of an authorization to manage radioactive sources must carry out periodic inventories of their sources at least once a year, to confirm their location and that they are secured in a certain location.

406. The Authorization Holders must ensure that each radioactive source or package of radioactive material is assigned the corresponding security category or security level, in accordance with that indicated in Annex I.

407. The protection of radioactive sources in use must be carried out according to their category and in accordance with the following levels of physical security:

a) Security level A, to prevent unauthorized removal of a source

b) Security level B, to minimize the probability of unauthorized removal of a source

c) Security level C, to reduce the probability of unauthorized removal of a source.

408. The general safety objectives for the use of radioactive sources that must be met at each assigned level are those established in Annex II.

409. The holders of the authorization for the use or storage of radioactive sources or those responsible for the transport of radioactive material must have physical security plans consistent with the Category and level of security, whose minimum content must include the specifications of Annex VI.

410. Physical security systems and means must be properly maintained to ensure compliance with their specifications and design objectives.

411. The authorization for the use of radioactive sources will be granted when it complies, in addition to the applicable radiological safety requirements, with the physical safety requirements applicable to the corresponding category and level of safety, duly supported by the respective documentation.

412. The Authorization Holders must establish appropriate measures so that the people involved with the radioactive source are alert to any suspicious behavior in relation, not only to the radioactive source and the property in which it is housed, but also to the immediate environment. , having to report such behaviors to the Authorization Holder, the local police and/or NATO.

413 Authorization holders must train their staff in relation to the physical security system established at their facility

5. SPECIFIC REQUIREMENTS IN THE USE OF RADIOACTIVE SOURCES

5.1 Responsibilities in the safety of sources

501. The Holder of authorizations for the use of radioactive sources classified in Category 1, 2 and 3 is responsible for compliance with the standard and must have and implement a physical security plan in accordance with the requirements of this standard and approved by NATO, having to carry out its review, in the event of a change in the conditions of the work environment, including any new information on the threat.

502. In the case of using Category 4 and 5 sources, the Authorization Holder must comply with the general radiological safety measures established in the regulations of Law No. 28028 and the provisions of the conditions and limits of its authorization.

Safety requirements for sources in Categories 1, 2 and 3

503. For all those classified in Categories 1, 2 and 3, the protection of the source must be ensured through the application of the security measures indicated in Annex III.

504. An evaluation of the level of threat must be carried out through a risk analysis process where the source is described, the nature of the activity, the environment in which the activity is carried out and the existing security measures, credible threats are identified in In relation to the activity and possible consequences of the threat, the effectiveness of the security measures to achieve the objective is evaluated initially, and in the review process, and additional or modified security measures are identified, if required, to achieve the objective.

5.1.2 Responsibilities for access

505. The people who are in charge of supervising the implementation of the standard and security plans, and the transportation of a source must previously undergo a basic security check in accordance with the provisions of paragraph 2 of Annex V.

506. The participation of any person in the physical security of a Category 1, 2 and 3 source must be justified, and their identity must be verified as indicated in paragraph 1 of Annex V.

507. Any person who is in the presence of a Category 1, 2 and 3 source, without having to do with its management, must be properly identified as indicated in paragraph 1 of Annex V, be accompanied by an authorized person and be under rigorous surveillance.

5.1.3 Knowledge of threat level

508. The Holder of the authorization must update the physical security provisions of the source in accordance with the provisions of the Security Plan of the source when he becomes aware of a change in the level of threat through communication from the National Police or NATO. .

5.1.4 Transfer and disposal of relevant sources

509. The Authorization Holder must not transfer ownership of the source or make its disposal without prior written approval from NATO.

5.1.5 Responsibilities of suppliers of services

510. When a technical service or maintenance is concluded, the physical security measures that have been temporarily disabled to perform the service must be restored, or, if they cannot be restored, the measures considered in the Security Plan must be applied to these cases.

5.1.6 Responsibilities of other people.

511. It must be ensured that no person interferes, removes, alters, damages or disables any physical security measure provided to secure a radioactive source, except that the removal, transport or technical service is carried out in accordance with the provisions of the Physical Security Plan. from the source.

512. No radioactive source should be abandoned under any circumstances, under the responsibility of the natural or legal person in charge of it.

513. The transfer of Category 1 or 2 sources should be carried out only when it has been approved by NATO.

5.2 Physical Security Measures during the use and storage

514. Physical security measures during the use and storage of radioactive sources must meet the requirements established in Annex III, in accordance with the security level assigned to a radioactive source.

a. Category 1 Sources

515. A Category 1 source, it must be protected during use and storage,

At a minimum, by physical security measures that provide sufficient delay to allow the immediate detection and evaluation of the intrusion, as well as the interruption of unauthorized removal by a private guard service or the National Police.

b. Category 2 sources

516. A Category 2 source must be protected during use and storage, at a minimum, by physical security measures that provide sufficient delay to allow immediate detection and evaluation of unauthorized access to the source.

c. Category 3 Sources

517. A Category 3 source must be protected during use and storage, at a minimum, by physical security measures capable of preventing unauthorized access to the source by human force.

5.2 Security measures by procedure

518. Sources must be protected by actions consistent with the security objectives prescribed in Table 1 of Annex IV, according to the level of existing threat and the Category of the source.

5.3 Security management

5.3.1 Threat level escalation

519. When the threat level increases, the security objectives must be increased to those corresponding to the highest threat level, within the time frame specified in the security plan.

5.3.2 Notification of a security breach

520. The Holder of the authorization and responsible for physical security must immediately notify the National Police and NATO of any violation of physical security that includes robbery, theft, unexplained loss, unauthorized damage, unauthorized access, unauthorized transfer or any other, and must provide, at a minimum, information on the circumstances of the event, the actions taken or planned to be taken to correct the violation, and any other information that may help in the recovery of the radioactive source in the event that it is lost or stolen. .

521. The Clearance Holder must submit to NATO a written incident report containing the information described in paragraph 520, within 7 days of the event notification date.

5.3.3 Accounting and registration

522. The Holder of the authorization must always be aware of the location of the radioactive sources under his charge.

523. Records must be kept on:

a) Detail of the location, serial number or identification number of the source, including a copy of the radioactive source certificate or other certification b) Detail of the physical and chemical composition of the isotope at the source

c) Construction details and type of radioactive source d) Activity and activity measurement date

e) Details of the import, export, transfer, disposal or change in the location of the radioactive source in the previous 12 months; and f) NATO authorizations for activities with the radioactive source

6. SPECIFIC REQUIREMENTS IN THE TRANSPORT OF RADIOACTIVE SOURCES

601. Security measures must be applied to the transport of radioactive sources in accordance with the corresponding security level as specified in Table D of Annex I.

602. The transport of radioactive sources whose security level is low must be carried out through the radiological security controls that normally apply to said material, with reasonable consideration of its physical security.

603. The authorization for the transport of radioactive sources, when applicable, will be approved after the corresponding physical security requirements have been met.

6.1 Measures for the basic level of security

604. The implementation of physical security measures must consider all information obtained regarding existing threats.

605. The transfer of the transported radioactive source must be carried out only to the holder of the authorizations or to persons duly authorized for reception.

606. In the case of temporary storage in transit locations, security measures similar to those for use and storage described in section 5.2 of this standard must be applied.

607. Action procedures must be available in case of delay in the delivery of the packaging with respect to the scheduled time.

608. Radioactive packages must be transported in secure, closed or covered vehicles. If the weight of a package is greater than 2000 kg, the transport can be carried out, duly insured, in an open vehicle and under additional requirements specifically established by NATO.

609. Persons involved in transportation must be properly trained about threats and their recognition, methods to deal with said threats and problems, as well as security plans in accordance with their responsibilities.

610. Every person who participates in the transport of radioactive sources must be positively identified as indicated in Annex V.

611. Carriers must conduct a physical security inspection of the vehicle or transport and ensure that these measures are maintained during transport.

612. Shippers must provide written instructions to transportation personnel on required security measures, including how to respond to a security incident.

613. The reliability of the personnel involved in the transport must be checked through a basic security examination, in accordance with the provisions of Annex V.

6.2 Measures for the high security level

614. Shippers and carriers transporting qualified sources at the high security level must register with NATO, before starting the first transport.

615. Shippers, carriers and receivers, as well as others involved in the transport of high security level radioactive sources, must adopt, implement and periodically review a physical security plan.

616. The sender must notify the recipient and NATO in advance of the planned shipment, the mode of transport and the expected time of arrival, and the recipient must confirm its ability and willingness to accept the shipment in the expected time.

617. The vehicle transporting the high security level radioactive source must be properly tracked during the transport of the material.

618. The carrier must have and provide, in the means of transport, the means for personnel to communicate with the point of contact specified in the security plan.

619. Continuous attention to the means of transportation must be maintained and, if this is not possible, it must be secured in an appropriate area in a way that meets detection and response requirements.

620. Persons involved in transportation must be adequately trained on threats, recognition and methods to deal with such threats and problems, as well as security plans in accordance with their responsibilities.

621. The transport of radioactive sources must be accompanied by duly instructed guards and NATO must be informed of this.

6.3 Transport security plan

622. To carry out the transport of the radioactive source of basic and increased level, a Transport Security Plan must be in place that contains the information indicated in section 2 of Annex VI and demonstrates the way in which the requirements of the standard are met. .

623. The Security Plan must be submitted to NATO at least 7 days before the expected date of shipment or, in the case of frequent shipments, the first shipment, for approval.

624. In the event of a change in the environment used for the Security Plan, including new credible threat information, it must be reviewed and submitted to NATO.

6.4 Security objectives to be met

a. Low security level 625.
During the transport of the low security level radioactive source, it must be protected, at a minimum, by physical security measures that prevent unauthorized access to the source by human force.

b. Basic security level

626. During the transport of the basic security level radioactive source, it must be protected, at a minimum, by physical security measures that provide sufficient delay to allow immediate detection and evaluation of unauthorized access to the source.

c. High security level

627. During the transport of the high security level radioactive source, it must be protected by physical security measures that provide sufficient delay to allow immediate detection and evaluation of the intrusion, as well as the interruption of unauthorized removal by part of a guard service or the police.

6.5 Compliance with the transport security plan

628. Compliance with the Safety Plan is the responsibility of the Authorization Holder and any person involved in the transport of radioactive material.

6.6 Operational requirements

629. In the regular transport of radioactive sources, scheduled routine movements must be avoided.

630. Routes with the possibility of natural disasters or where there is civil disorder or known threats should be avoided.

631. In the transport of high security radioactive sources, alternate routes must be identified in advance.

632. The total transportation time, the number of intermodal transfers and the time between intermodal transfers should be kept to the minimum necessary.

633. Advance information regarding transportation and the physical security measures to be applied must be restricted to a minimum number of people.

634. Vehicles with radioactive packages and radioactive packages must not be left unattended for any reason.

6.7 Notification requirements

635. The sender, carrier and/or receiver of the radioactive source must immediately notify the police and NATO of any breach of physical security that includes theft, detectable theft, unexplained loss, unauthorized access, unauthorized transfer or any other another, must provide, at a minimum, information on the circumstances of the event, the countermeasures carried out or actions planned to recover the material or correct the violation, and any other information that may help in the recovery of the radioactive source that is lost or stolen.

636. The sender or receiver of a radioactive source must submit to NATO a written report of the incident containing the information described in 635, within 7 days of the date of notification of the event.

6.8 International transport

637. The international shipment of radioactive packages from Category 1 and 2 radioactive sources, with high and medium security levels, must be carried out in such a way that the requirements of this standard are maintained until the radioactive package crosses the border, also complying with the requirements for exporting fonts.

7. VERIFICATION OF COMPLIANCE AND APPLICATION OF SANCTIONS

701. NATO will monitor compliance with the specific physical security provisions prescribed in this standard.

702. Failure to comply with the provisions of this standard and other specific provisions that NATO dictates will be sanctioned in accordance with the regime established in the Regulations of Law No. 28028 (DSN No. 0392008EM).

ANNEX I

Table A. Categorization of radioactive sources

Category	radioactive source	A/D 1	Security level
1	Radioisotope thermoelectric generators (RTGs) irradiators teletherapy sources Multiple sources of teletherapy (gamma knife)	1000ÿ A/D	A
two	Industrial gamma radiography sources High Dose Rate Brachytherapy Sources	1000>A/Dÿ10	B.
3	Fixed industrial meters with high activity sources Well Logging Sources	10>A/Dÿ1	C
4	Low dose rate brachytherapy sources (except plates of eyes and permanent implants) Industrial meters that do not incorporate sources of high intensity bone densitometers Static eliminators	1>A/Dÿ0.01	Are applied measures general of security radiological
5	Low dose rate eye plates and permanent implants X-ray fluorescence devices electronic capture devices Mossbauer spectroscopy sources PET Checkup Supplies	0.01>A/D and A > exempt	

1 A is the activity of the source and D is the level of relative danger (Dvalue), indicated in Table B. For sources or uses not included in the indicated tables, NATO will provide the corresponding values.

Table B. Relative hazard level D 1 by radionuclide

radionuclide	D-value (GBq)	radionuclide	D-value (GBq)
Americium 241	60	Nickel 63	6x10 4
Americium 241/Be	60	Palladium 103	9x10 4
Cadmium 109	2 x 10 4	phosphorus 32	1x10
Cesium 137	100	Plutonium 238	4 60
Californium 252	twenty	Plutonium 239/Beryllium	60
Cobalt 57	700	Polonium 210	60
Cobalt 60	30	Prometheus 147	4x10 4
Curium 244	fifty	Radius 226	40
Gadolinium 153	1x10	Ruthenium 106 (Rhodium 106)	300
Germanium 68	3 700	Selenium 75	200
gold 198	200	Strontium 90 (Yttrium 90)	1x10
Iodine 125	200	Technetium 99m	3 700
Iodine 131	200	Thallium 204	2x10 4
Iridium 192	80	Thulium 170	2x10 4
iron 55	8x10 5	Tritium (H3)	2x10 6
Krypton 85	3x10 4	Ytterbium 169	300
Molybdenum 99	300		

1 For isotopes not included in the Table, contact NATO for the applicable D-value.

The categorization of a source aggregation will be determined:

a) For aggregation of sources of the same radionuclide, it is the sum of the activities (their level of danger): A_i) divided by D

$$(A/D) = (\ddot{y}iAi \quad /D)$$

b) For aggregation of sources of different radionuclides, it is the sum of activities of each radionuclide $_n$, (Ai,n) divided by the level of danger of each radionuclide (Dn)

$$(A/D) \quad = (\ddot{y}iAi,1 / D1) + (\ddot{y}iAi,2 / D2) + \ldots \ldots + (\ddot{y}iAi,n / \quad Dn)$$

Table C. Safety thresholds for transport

radionuclide	security threshold (GBq)	radionuclide	security threshold (GBq)
Americium 241	600	Palladium 103	9x10 5
Americium 241/Be	600	Plutonium 238	600
Cadmium 109	2 x 10 5	Plutonium 239/Beryllium	600
Cesium 137	1000	Polonium 210	600
Californium 252	200	Prometheus 147	4x10 5
Cobalt 57	7000	Radius 226	400
Cobalt 60	300	Ruthenium 106 (Rhodium 106)	3000
Curium 244	500	Selenium 75	2000
iron 55	8x10 8	Strontium 90 (Yttrium 90)	1x10 4
phosphorus 32	1.5x10 6	Thallium 204	2x10 5
Gadolinium 153	1x10 4	Technetium 99	2.7x10 6
Germanium 68	7000	Tritium 3	1.2x10 8
Iridium 192	800	Thulium 170	2x10 5
Krypton 85	3 x 10 7	Iodine 125	9x10 6
Molybdenum 99	1.8 x 10 6	Iodine 131	2.1x10 6
Nickel 63	6 x 10 5	Ytterbium 169	3000
gold 158	1.8 x 10 6		

(*) For isotopes not included in the Table, contact NATO for the applicable value.

Table D. Safety levels in radioactive source transport

packaging	Security level
Remissions of packages of radioactive sources excepted according to the Regulation for the Safe Transport of Radioactive Materials of the IAEA, not exceeding the activity of material in non-special form and radioactive material specified as BAE1 and OCSI	Bass
Shipments that include packages containing radioactive materials that are not exceed the thresholds in Table C	Essential
Shipments comprising at least one package containing material radioactive equal to or greater than the thresholds in Table C	Tall

ANNEX II

Physical security functions and objectives

FUNCTIONS OF PHYSICAL SECURITY	PHYSICAL SECURITY OBJECTIVES		
	SECURITY LEVEL A	SECURITY LEVEL B	SECURITY LEVEL C
Detection	Immediately detect any unauthorized access to the source or protected area		
	detect immediately any unauthorized removal attempts from the source, including those made by personnel from the same facility. Immediately assess	Detect any unauthorized removal attempt of the radioactive source	Detect unauthorized removal of the radioactive source
	detection Immediately notify response		
	personnel Have means to detect loss of source by		
	verification Create sufficient delay Create sufficient delay after detection to minimize		
Time delay	possibility for unauthorized removal personnel response interrupt and prevent	unauthorized removal	Create delay to reduce the possibility of unauthorized withdrawal
Response	Respond immediately to an assessed alarm with sufficient resources to disrupt and prevent unauthorized removal	Immediately initiate response to interrupt unauthorized withdrawal	Takes appropriate action in the event of an unauthorized removal of a source.
Physical security management	Establish access controls at the source location that effectively restrict access to authorized persons only		
	Ensuring the probity of authorized persons		
	Identify and protect sensitive information		
	Develop a physical security plan		
	Ensure that there is capacity to handle events that compromise the physical security covered by the security contingency plan		
	Establish a reporting system for events that compromise physical security		

ANNEX III

Security measures to apply according to level

security level A

security function	security objective	Security measures
Detection	Immediately detect any unauthorized access to the protected area/source	Electronic intrusion detection system and/or continuous surveillance by the operating personnel.
	Immediately detect any unauthorized source removal attempts, including acts by insiders	Electronic tamper detection equipment and/ or continuous surveillance by operator personnel Remote CCTV system monitoring or evaluation by operator/
	Immediately assess detection	response personnel
	Immediately notify responders Fast, reliable means of communication	and miscellaneous such as telephones, cell phones, pagers, radios Daily verification
	Identify a way to detect the loss of a source through verification	through physical checks, CCTV, tampering detection devices, etc.
Time delay	Create a sufficient delay after detection so that responders can interrupt the unauthorized removal	Systems of at least two layers of barriers (eg, walls, confinements) that together produce sufficient delay for responders to stop the event
Response	Respond immediately to an assessed alarm with sufficient resources to disrupt and prevent unauthorized removal	Immediate response capacity with the number of people, equipment and training to stop the event
Security management	Establish access controls at the source location to allow only authorized persons to enter	Identification and verification, e.g. lock controlled by card reader and personal code, or key and key control
	Ensuring authorized persons are trustworthy	Background check for all personnel authorized to enter unaccompanied to the location of the source or access to sensitive information
	Identify and protect sensitive information	Procedures to identify sensitive information and protect it from unauthorized disclosure
	Develop a security plan	Security plan that complies with regulations and responds to increasing threat levels
	Ensure that there is capacity to handle situations that compromise security covered in security contingency plans	Procedures for responding to situations that compromise safety
	Establish a notification system for situations that compromise safety	Procedures for timely notification of situations that compromise safety

Security level B

security function	security objective	Security measures
	Immediately detect any unauthorized access to the protected area/source	Electronic penetration detection system and/ or continuous surveillance by the operating personnel.
	Detect any unauthorized withdrawal attempts from the source.	Electronic tamper detection equipment and/ or continuous surveillance by operator personnel Remote monitoring of CCTV system or
	Immediately assess detection	

Detection		evaluation by the operator / response personnel
	Immediately notify responders Fast, reliable means of communication	and miscellaneous such as telephones, cell phones, pagers, radios Weekly verification
	Identify a way to detect the loss of a source through verification	through physical checks, CCTV, tampering detection devices, etc.
Time delay	Create a delay to minimize the chance of the unauthorized withdrawal occurring	Two-layer barrier systems (eg, walls, confinements) Equipment and procedures to initiate an immediate
Response	Immediately initiate a response to stop the unauthorized withdrawal	response An identification measure
Security management	Establish access controls at the source location to allow only authorized persons to enter	
	Ensuring authorized persons are trustworthy	Background check for all personnel authorized to enter unaccompanied to the location of the source or access to sensitive information
	Identify and protect sensitive information	Procedures to identify sensitive information and protect it from unauthorized disclosure
	Develop a security plan	Security plan that complies with regulations and responds to increasing threat levels
	Ensure that there is capacity to handle situations that compromise security covered in security contingency plans	Procedures for responding to situations that compromise safety
	Establish a notification system for situations that compromise safety	Procedures for timely notification of situations that compromise safety

Security level C

Function of security	security objective	Security measures
Detection	Detect any unauthorized withdrawal from the source	Improper manipulation detection equipment and/or periodic surveillance by operating personnel.
	Immediately assess detection	Assessment by operator/response personnel Monthly verification by physical checks, tamper
	Identify a way to detect the loss of a source through verification	detection devices, or others that confirm the presence of the source One-barrier systems (e.g., box, source housing) or under observation of the source operating personnel Procedures identify the necessary actions in
Time delay	Create a delay to minimize the possibility of unauthorized withdrawal	accordance with the contingency plans An identification measure
Response	Implement appropriate actions in the event of unauthorized removal of the source	
Security management	Establish access controls at the source location that effectively restrict access to authorized persons only	
	Ensuring authorized persons are trustworthy	Background check for all personnel authorized to enter unaccompanied to the source location and access to sensitive information
	Identify and protect sensitive information	Procedures to identify sensitive information and protect it from unauthorized disclosure
	Develop a security plan	Documentation with provisions of

		safety and referral procedures
	Ensure the ability to handle security-compromising situations covered in security contingency plans	Procedures for responding to situations that compromise safety
	Establish a notification system for situations that compromise safety	Procedures for timely notification of situations that compromise safety

ANNEX IV

Administrative and procedural security requirements

Table IV:1. Scale of Security and Procedural Requirements with respect to the level of threat for a source of Category 1, 2 and 3

Category	THREAT LEVEL		
	Low, Very low or Insignificant	Medium	high or extreme
1	A,D	A,B,D,E	A B C D E
2	A	A,B,D,E,	A B C D E
3	A	A,B	A B C D E

Table IV. 2 Security actions for Table IV .1.

Cluster	security action
A	Annual review of security plans
	Annual review of intrusion detection, evaluation of events and averages of communication
	Annual review of access controls and physical barriers
	Annual review of staff access requirements
	Review of the process of transfer, removal or withdrawal of source
	Annual inductive talk to staff on security awareness
	Talk to specific staff about security awareness
	Annual audit of all sources
	Accounting or monthly check to confirm presence of sources
	Visitors must sign in and be escorted while present inside of the security area defined in the Security Plan
B.	Accounting or weekly check to confirm presence of source
C	Visitors not allowed to enter within the secure area defined in the Plan, unless unless authorized by NATO, police service, security service ambulance or fire brigade
	Delivery of items to be dispatched and received outside the site with movement of items, performed only by personnel who meet the requirements of the paragraph 507.
	Semi-annual talks to staff on security awareness
	Accounting or daily check to confirm presence of the source
D	Annual exercise of response arrangements of the guard or police service
AND	Semi-Annual Staff Access Review

ANNEX V

Identity verification and physical security control

1. Provisions for carrying out an identity check

a) The identity of any person who will have access to a relevant physical security source must be verified by means of: National Identity Document (DNI or Foreign Passport or Residency Document) Confirmation of employment history, education and personal references As required considers necessary, obtaining independent information to corroborate that provided by the person (references)

b) Every person who has access to a relevant security area must provide the document corresponding original for this purpose.

2. Basic security check

In addition to the identity check, the person must have a basic security review, which includes a security evaluation issued by the National Police of Peru and a criminal record check issued by the Judicial Power.

ANNEX VI

Content of the Security Plan 1. Storage and use of sources

The Plan must contain:

a) Description of the source (isotope, activity, date of measurement, serial number and chemical physical form) b) Description of the practice and use of the source, as well as its Category. c) Description of the location of the source in the facility or area where it is used or stored, including a plan, the security measures used to protect the source and definition of the security area.

d) Assignment of responsibilities and personnel qualification e)

Description of security threats (robbery, theft or sabotage, mechanical or electronic failure of the security system) f) Description of the security measures to be used to meet the requirements of the standard, including access control, key control, CCTV surveillance, personal surveillance, identity checks and basic security of personnel, inventories and records related to source management, information security, procedures before, during and after maintenance, contingency response arrangements including breach notifications, security education and awareness, actions to be taken upon change in threat level, provisions for periodic review and modification of the security plan.

2. Transportation of sources

The Plan must contain:

a) Description of the source to be transported (isotope, activity, date of measurement, serial number and form physical chemical, transport packaging, source category) b)

Statement of the purpose or justification for the transport of the source c)

Description of the vehicle in which the source will be transported and the provisions to ensure the boarding during transfers or other stops en route d) Assignment

of responsibilities and qualification of personnel e) Name, address

and activity, and out-of-hours contact details for sender, receiver, carrier and, where used, guard or police f) Description of security threats (burglary, theft or sabotage, mechanical or electronic failure of the security system)

g) Description of the security measures to be used to satisfy the requirements of the standard
h) Description of the security procedures to be applied to satisfy the security requirements of the standard, including arrangements for notifying authorities (NATO, police or other local), contingency or emergency procedures for vehicular accidents or violations including, for Category 1 sources, a planned primary and alternate route, response arrangements of security including notification of security breaches, security information to individuals involved in the transport that includes the threat, threat level, and response arrangements for contingencies, identity checks and basic security of personnel, physical security information, means of communication between parties involved in the transport, actions to be taken in case of threat level change.
i) Provisions for periodic review and modification of the security plan.

REFERENCES

[1] IAEA. Security of Radioactive Sources. Nuclear Security Series No. 11. 2009

[2] IAEA. Security in the Transport of Radioactive Material. Nuclear Security Series No. 9. 2008

[3] ARPANSA. Security of Radioactive Sources. Code of Practice. Radiation Protection Series No. 11. 2007

[4] IAEA. Revised Code of Conduct on the Security and Safety of Sources Radioactive. IAEA/CODEOC/2004/Rev.1 2007

[5] IAEA. Regulations for the Safe Transport of Radioactive Material – 2009 Edition. Safety Requirements No. TSR1. 2009.

[6] IAEA. Categorization of Radioactive Sources, IAEA Safety Standards Series No. RSG1.9. Vienna, 2005.

[7] IAEA. Terminology Used in Nuclear Safety and Radiation Protection. IAEA Safety Glossary. 2007.