UNIVERSIDAD NACIONAL
SISTEMA DE ESTUDIOS DE POSGRADO
FACULTAD DE FILOSOFÍA Y LETRAS
ESCUELA DE LITERATURA Y CIENCIAS DEL LENGUAJE
MAESTRÍA PROFESIONAL EN TRADUCCIÓN (INGLÉS-ESPAÑOL)

Estrategias adecuadas de documentación para la traducción de guías de seguridad física de fuentes radiactivas

Trabajo de investigación para aspirar al grado de
Magíster en Traducción Inglés-Español

presentado por

Néstor Eladio Peña Rodríguez

Cédula No. 6-0388-0928

2017

Nómina de participantes en la actividad final
del trabajo de graduación

Estrategias adecuadas de documentación para la traducción de guías de seguridad física de fuentes radiactivas

presentado por el sustentante
NÉSTOR ELADIO PEÑA RODRÍGUEZ
el día
3 de junio de 2017

Personal académico calificador:

M.A. Meritxell Serrano Tristán _____
Profesora encargada
Seminario de Traductología III

M.A. Adriana Castro Benítez _____
Profesora tutora

M.A. Allan Pineda _____
Coordinador
Plan de Maestría en Traducción

Sustentante:
Néstor Eladio Peña Rodríguez _____

Nota aclaratoria

La traducción que se presenta en este tomo se ha realizado para cumplir con el requisito curricular de obtener el grado académico de Maestría en Traducción Inglés–Español, de la Universidad Nacional.

Ni la Escuela de Literatura y Ciencias del Lenguaje de la Universidad Nacional, ni el traductor, tendrá ninguna responsabilidad en el uso posterior que de la versión traducida se haga, incluida su publicación.

Corresponderá a quien desee publicar esa versión gestionar ante las entidades pertinentes la autorización para su uso y comercialización, sin perjuicio del derecho de propiedad intelectual del que es depositario el traductor. En cualquiera de los casos, todo uso que se haga del texto y de su traducción deberá atenerse a los alcances de la Ley de Derechos de Autor y Derechos Conexos, vigente en Costa Rica.

Resumen

Este trabajo consiste en la traducción al español de una guía creada por el Organismo Internacional de Energía Atómica (OIEA) para la protección de fuentes radiactivas y el análisis de los métodos de documentación adecuados para su realización. Las razones para realizar este trabajo surgen a partir del reconocimiento de que existe un vacío sobre estudios que aborden el uso de la documentación aplicada a la traducción de textos técnicos, particularmente los relacionados con fuentes radiactivas. Se utiliza como base la recomendación de varios expertos en documentación y traducción para proponer estrategias útiles en la traducción de la guía en estudio. A partir de la teoría, se propone un método compuesto por varias estrategias documentales que se listan a continuación: conocer el sistema de publicaciones del OIEA, identificar las necesidades informativas terminológicas, temáticas y referenciales que plantea el texto, realizar una búsqueda en línea de fuentes documentales que ayuden a resolver tales necesidades, evaluar las fuentes encontradas y crear fichas descriptivas que documenten dicha evaluación. El trabajo concluye que es posible aplicar distintas estrategias documentales para mejorar los procesos de traducción, pero que estas estrategias deberán ser adaptadas a cada texto por traducir.

Palabras clave: documentación, fuentes radiactivas, traducción, OIEA

Abstract

This research consists of the translation into Spanish of a guide developed by the International Atomic Energy Agency (IAEA) for the protection of radioactive sources, and the analysis of the appropriate documentation strategies to be applied to the translation process. The need for researching this topic comes from the realization that there is insufficient literature addressing the use of documentation strategies in the translation of technical texts, particularly, the ones related to radioactive sources. The recommendations of experts in documentation and translation serve as the basis for proposing strategies that are useful in the translation of the abovementioned guide. Based on the theory, the method proposed includes the following strategies: looking into the IAEA's publication system; identifying in the text the needs regarding terminology, subject matter, and reference system; finding online bibliographic sources that could solve the identified needs; evaluating those sources; and, creating fact sheets to document the evaluation. This investigation concludes that it is possible to apply different documentation strategies that will improve the translation process. However, these strategies need to be adapted to each text to be translated.

Keywords: documentation, radioactive sources, translation, IAEA

Índice general

Traducción

1. Introducción

1.1. Antecedentes

Esta guía formula orientaciones para la aplicación de medidas de seguridad física en las fuentes radiactivas. Además, brinda consejos para la implementación de las disposiciones relacionadas con la seguridad física que se describen en el *Código de conducta sobre seguridad tecnológica y física de las fuentes radiactivas* [1] (en adelante denominado el *Código de Conducta*) (en la sección Definiciones se explican los términos empleados en esta publicación).

Si bien esta guía de implementación reemplaza al documento titulado *Security of Radioactive Sources (Interim Guidance for Comment)* (IAEA-TECDOC-1355) [2], se toma en consideración el enfoque general de seguridad física establecido en dicha publicación, el cual pudo haberse usado como referencia por algunos Estados en la elaboración de sus regímenes de seguridad física. Esta publicación fue armonizada con la *Clasificación de las fuentes radiactivas del OIEA* [3] y propone un enfoque graduado para la seguridad física con base en un conjunto de niveles de seguridad física y las funciones de disuasión, detección, demora, respuesta y gestión de la seguridad física.

Esta publicación debe leerse en conjunto con los siguientes documentos: *Código de Conducta* [1], *Clasificación de las fuentes radiactivas* [3]*, Seguridad de los generadores de radiación y de las fuentes radiactivas selladas* [4], *Normas básicas internacionales de seguridad para la protección contra la radiación ionizante y para la seguridad de las fuentes de radiación* [5] y *Principios fundamentales de seguridad del OIEA* [6].

Finalmente, esta guía reconoce que debe existir un balance entre gestionar las fuentes en condiciones de seguridad física y permitir que el personal autorizado haga uso de ellas en condiciones de seguridad radiológica. Puesto que las fuentes radiactivas son una herramienta

integral y esencial para las industrias de la salud, la manufactura, la investigación y el control de calidad en todo el mundo, se debe procurar que los múltiples beneficios del uso de las fuentes no sean obstaculizados indebidamente. El desafío para la autoridad reguladora, los usuarios y otras partes interesadas es encontrar el balance correcto.

1.2. Objetivo

El objetivo de esta guía es que sea utilizada por los Estados en la formulación de políticas de seguridad física para las fuentes radiactivas y por las autoridades reguladoras en la elaboración de requisitos de seguridad física que sean acordes con el *Código de Conducta*. También ayudará a los Estados contraparte a cumplir algunas de las obligaciones suscritas bajo el *Convenio internacional para la represión de los actos de terrorismo nuclear* [7]. También puede ser útil para los operadores de fuentes radiactivas en la elaboración de sus programas de seguridad física.

1.3. Alcance

Esta guía incluye orientaciones y medidas recomendadas para la prevención, detección y respuesta ante actos dolosos que involucren fuentes radiactivas; además, ayudará a prevenir que se pierda el control sobre dichas fuentes. No cubre el material nuclear según se define en la *Convención sobre la protección física de los materiales nucleares* y su respectiva enmienda [8], excepto el caso de las fuentes que contengan Plutonio-239.

Si bien esta publicación no aborda específicamente la seguridad física del material radiactivo no sellado, el Estado puede decidir aplicar a dicho material los conceptos y las medidas de seguridad aquí señaladas.

Esta guía recomienda que se apliquen medidas de seguridad a las fuentes radiactivas en su fabricación, uso y almacenamiento a corto o largo plazo (ver la sección Definiciones).

Este documento recomienda que las medidas de seguridad se apliquen con un enfoque graduado, tomando en consideración la evaluación de la amenaza actual, la atractividad

relativa de la fuente y las posibles consecuencias de su uso doloso. El nivel de seguridad requerido se obtiene mediante la combinación de disuasión, detección, demora, respuesta y gestión de la seguridad física.

Los Estados podrían decidir que algunas o todas sus fuentes tienen un nivel de riesgo menor o mayor que el indicado en esta publicación. En tales casos, los Estados deberán tener la flexibilidad para cambiar las medidas de seguridad en casos necesarios, con base en las medidas recomendadas en este documento. Al hacerlo, deberán mantener, en la medida de lo posible, la estructura general presentada en esta guía.

Esta publicación no incluye recomendaciones sobre la preparación y respuesta ante emergencias o la intervención o remediación de zonas contaminadas. Tal información está disponible en otras publicaciones del OIEA [5, 9, 10]. La guía sobre cómo proteger a las personas de la radiación después de un ataque las proporciona la Comisión Internacional de Protección Radiológica [11].

Finalmente, este documento no aborda el transporte de material radiactivo, incluidas las fuentes radiactivas. Tales orientaciones, junto con lo referente a transportistas subsidiarios, están indicados en la Ref. [12].

2. Responsabilidades del Estado y del operador

2.1. Introducción

El *Código de Conducta* [1] reconoce que un sistema nacional de control regulatorio eficaz sienta las bases para la seguridad física y radiológica de las fuentes radiactivas en un Estado. Esta sección brinda orientación adicional sobre las responsabilidades del Estado y del operador en relación con la seguridad física de las fuentes radiactivas.

2.2. Estado

Cada Estado deberá definir su amenaza interna (ver Sección 3.8.1). Este proceso debe iniciar con una evaluación de la amenaza nacional, la cual consiste en un análisis que documenta, a nivel nacional, las motivaciones, intenciones y capacidades verosímiles de posibles adversarios que puedan causar daño a través del sabotaje de una instalación o el retiro no autorizado de una fuente radiactiva para propósitos dolosos. Las orientaciones sobre este tema se comentan a fondo en la Ref. [13].

Cada Estado deberá tomar las medidas necesarias para garantizar que las fuentes radiactivas dentro de su territorio, o bajo su jurisdicción o control, estén protegidas en condiciones de seguridad física durante y al final de su vida útil. Esto incluye la promoción de una cultura de la seguridad física para las fuentes radiactivas, así como la educación y capacitación adecuadas para los reguladores y los operadores.

Los Estados deberán tener en vigor una infraestructura legislativa y regulatoria nacional eficaz que rija la seguridad física de las fuentes radiactivas, la cual:

— prescriba y asigne responsabilidades gubernamentales a los organismos correspondientes, incluida una autoridad reguladora independiente que establezca, aplique y mantenga un régimen que garantice la seguridad de las fuentes radiactivas

— establezca los requisitos de seguridad física para las fuentes radiactivas e incluya un sistema de evaluación, adjudicación de licencias y verificación de cumplimiento u otros procedimientos para la concesión de permisos

— designe a los operadores como los principales responsables de la seguridad física de las fuentes radiactivas

— brinde las medidas para reducir la posibilidad de intentos de actos dolosos

— brinde las medidas para mitigar o minimizar las consecuencias de los actos dolosos que involucren fuentes radiactivas

— establezca delitos sancionables que incluyan los actos dolosos que involucren fuentes radiactivas.

La aplicación y la ejecución de la infraestructura legislativa y regulatoria para las fuentes radiactivas dependen de la cooperación eficaz entre los diferentes organismos a los que se les asignen responsabilidades gubernamentales. Normalmente, estos organismos incluyen una autoridad reguladora, una comunidad de inteligencia, los ministerios del interior, de defensa, de transporte y de relaciones exteriores, fuerzas policiales, aduanas y guardia costera, así como otras entidades con responsabilidades asociadas a la seguridad.

Los Estados deberán garantizar que la autoridad reguladora cuente con los recursos apropiados, en personal y financiamiento, para cumplir con sus funciones regulatorias, incluida la implementación de un programa de inspección para verificar que la seguridad de las fuentes radiactivas se conserve eficazmente. El programa de inspección deberá estar sustentado por procedimientos escritos y ejecutado por personal calificado. La frecuencia de tales inspecciones deberá tomar en cuenta los niveles de seguridad (ver Sección 4.1) de las fuentes radiactivas y podría considerar el desempeño del operador en el cumplimiento de los requisitos de seguridad en el pasado. Las inspecciones sobre las medidas de seguridad física implementadas por el operador pueden realizarse junto con inspecciones que verifiquen el cumplimiento de otros requisitos regulatorios, tales como la seguridad radiológica o inspecciones particulares.

2.3. Operadores

Los operadores, como organismos autorizados, deberían ser los principales responsables de aplicar y mantener las medidas de seguridad física para las fuentes radiactivas conforme a los requisitos a nivel nacional. Los operadores podrían, dependiendo de los requisitos regulatorios establecidos por el Estado, designar o contratar a terceros para llevar a cabo las acciones y tareas relacionadas con la seguridad física de las fuentes

radiactivas. Sin embargo, el operador autorizado debería seguir siendo el principal responsable de velar por el cumplimiento de los reglamentos y la eficacia de las acciones y tareas realizadas. Además, los operadores deberían garantizar que su personal y contratistas estén debidamente capacitados y que cumplan con los requisitos reglamentarios, incluida la probidad.

Los operadores deberán verificar en intervalos establecidos que las fuentes estén en la ubicación autorizada. Cualquier ausencia o anomalía debería ser investigada y reportada de manera oportuna a la autoridad reguladora. Debería contarse con procesos que garanticen que se pueda identificar y rastrear todas las fuentes de categorías 1, 2 y 3 (ver Sección 4.2.1) para las cuales los operadores tengan autorización.

Cuando las autoridades reguladoras lo soliciten, los operadores deberán realizar pruebas de vulnerabilidad (ver la sección Definiciones) de sus fuentes radiactivas de acuerdo con la evaluación de la amenaza vigente.

Los operadores deberían promover una cultura de la seguridad física (ver Sección 3.2) y establecer un sistema de gestión de fuentes acorde con los niveles de seguridad (ver Sección 4.1) para garantizar que:

— se establezcan políticas y procedimientos que consignen alta prioridad a la seguridad física

— se identifiquen y corrijan oportunamente problemas que afecten la seguridad física según su importancia

— se establezcan claramente las responsabilidades en materia de seguridad física y se capacite, califique y compruebe debidamente la probidad de cada persona

— se definan claramente los niveles de autoridad para las decisiones relacionadas con la seguridad física

— se establezcan acuerdos institucionales y líneas de comunicación que se traduzcan en un adecuado flujo de información en materia de seguridad física para toda la organización

— se identifique y proteja la información sensible de acuerdo con las reglamentaciones nacional

— se gestionen las fuentes radiactivas de acuerdo con un plan de seguridad física (ver la sección Definiciones) cuando así lo solicite la autoridad reguladora

3. Conceptos de seguridad física

3.1. Introducción

Esta sección introduce los principios básicos aplicables a la seguridad física de las fuentes radiactivas establecidos en el Código de Conducta [1] y explica los conceptos de seguridad física, incluidas las funciones básicas: disuasión, detección, demora, respuesta y gestión de la seguridad física (Cuadro 1).

3.2. Cultura de la seguridad física

Debe existir una cultura de la seguridad física dinámica y eficaz en todos los niveles del personal y de la administración con que cuente el operador.

La cultura de la seguridad física son las creencias, actitudes, comportamientos y sistemas de gestión que, de manera conjunta y apropiada, conducen a una seguridad física más eficaz.

La base de la cultura de la seguridad física es que quienes cumplen un papel en la regulación, gestión u operación de instalaciones o actividades que involucren fuentes radiactivas, incluso quienes se ven afectados por estas actividades, reconozcan que existe una amenaza creíble y que la seguridad física es importante.

Quienes lean esta publicación también deben leer el documento llamado Nuclear Security Culture [14], que describe los conceptos y elementos básicos de la cultura de la seguridad física.

Cuadro 1. Principios del Código de Conducta para la seguridad física de las fuentes radiactivas [NT]

El Código de Conducta establece principios básicos aplicables a la seguridad física de las fuentes radiactivas, varios de los cuales son de relevancia para esta guía. De acuerdo con estos principios, todo Estado debe:

- Adoptar las medidas adecuadas y necesarias para garantizar que las fuentes radiactivas estén **"protegidas en condiciones de seguridad física durante su vida útil y al final de esta"** (párrafo 7).
- Recalcar "a los diseñadores, los fabricantes (tanto fabricantes de fuentes radiactivas como de dispositivos que contienen tales fuentes), los proveedores, los usuarios y quienes gestionan las fuentes en desuso **sus responsabilidades en lo que respecta a la seguridad física de las fuentes radiactivas**" (párrafo 15).
- Definir "su **amenaza interna** y **evaluar su vulnerabilidad** frente a dicha amenaza con respecto a las distintas fuentes utilizadas en su territorio, con base en la posibilidad de pérdidas de control o actos dolosos que involucren una o varias fuentes radiactivas" (párrafo 16).
- Implementar legislaciones y reglamentos que especifiquen los "requisitos en materia de **seguridad física encaminados a disuadir, detectar y demorar** el acceso no autorizado a fuentes radiactivas, así como el robo, pérdida, uso o retiro no autorizado de esas fuentes durante todas las etapas de gestión" (párrafo 19).
- Garantizar que "la autoridad reguladora establecida por su legislación tenga facultades para establecer condiciones claras y explícitas con respecto a las autorizaciones que expida, incluidas las condiciones relacionadas con:…(viii) las medidas para determinar, según corresponda, la **probidad** de las personas involucradas en la gestión de las fuentes radiactivas y (ix) el **carácter confidencial de la información** relacionada con la seguridad física de las fuentes radiactivas" (párrafo 20);
- Asegurar que la autoridad reguladora tenga facultades para **exigir que se presente un plan o evaluación de seguridad física, según corresponda, y promover el establecimiento de una cultura de la seguridad física** entre todas las personas y organismos involucrados en la gestión de las fuentes radiactivas (párrafos 20 y 22).

La cultura de la seguridad física podría mejorarse mediante varias acciones, según corresponda:

[NT] Notal del traductor (en adelante NT): Estos principios fueron tomados del *Código de conducta*

— asignar a un jefe de personal como responsable de la seguridad física de las fuentes radiactivas, pero a la vez garantizar que todo el personal esté consciente de que la seguridad física es una responsabilidad compartida por todos los miembros de la organización

— documentar las responsabilidades legales y regulatorias del operador en materia de seguridad física y hacérselo saber a los directores y al personal pertinente y, según corresponda, a todos los empleados y contratistas

— garantizar el reconocimiento de la amenaza y la capacitación de los directores, el personal de respuesta y toda persona con responsabilidades secundarias en materia de seguridad física

— abordar asuntos relacionados con la seguridad física en cursos de inducción para el personal y los contratistas

— dar instrucciones y brindar sesiones informativas para concientizar al personal y a los contratistas sobre la seguridad física, así como ofrecer capacitaciones y hacer evaluaciones de las lecciones aprendidas

— realizar pruebas de desempeño y mantenimiento preventivo periódicamente

3.3. Propósito de un sistema de seguridad

Los profesionales en materia de seguridad física a disposición del operador deberían ser los encargados diseñar un sistema de seguridad física que cumpla con la misión de disuadir a los adversarios de cometer actos dolosos o de minimizar a través de la detección, la demora y la respuesta las posibilidades de que logren consumar tales actos. Un acto doloso consiste en una serie de acciones llevadas a cabo por uno o varios adversarios (amenaza) para obtener acceso a una fuente (blanco) con la meta de cometer un acto de sabotaje u otro acto doloso, o bien para retirar la fuente sin autorización.

3.4. Funciones de seguridad física

Un sistema de seguridad física para proteger a las fuentes radiactivas de adversarios que intenten cometer actos dolosos debería diseñarse de manera que cumpla con las funciones básicas de seguridad: disuasión, detección, demora, respuesta y gestión de la seguridad:

— La ***disuasión*** ocurre cuando un adversario, de alguna manera motivado a llevar a cabo un acto doloso, es disuadido de hacer el intento. Las medidas de disuasión tienen el efecto de convencer al adversario de que intentar realizar el acto doloso sería muy difícil, que la posibilidad de éxito es muy incierta o que las consecuencias para el adversario serían muy negativas. Por lo tanto, las medidas que se toman específicamente para disuadir involucran hacerle saber al adversario que existen otras medidas que cumplen el resto de las funciones de seguridad física. Si esta acción logra el efecto deseado, el resultado es la disuasión.

— La ***detección*** consiste en descubrir que se intentó o se dio una intrusión que podría tener como objetivo el retiro no autorizado o sabotaje de una fuente radiactiva. La detección se logra mediante la observación, las cámaras de video, los sensores electrónicos, los registros de contabilidad, los sellos u otros dispositivos de detección de forzamiento, los sistemas de monitoreo y otros medios. El hecho de que los adversarios estén al tanto de las medidas de detección también puede servir de disuasión.

— La ***demora*** impide que un adversario logre el acceso no autorizado a una fuente radiactiva, o su retiro o sabotaje, generalmente por medio de barreras u otros obstáculos físicos. Una medida de demora es el tiempo, después de la detección, que requiere un adversario para retirar o sabotear una fuente. El hecho de que los adversarios estén al tanto de las medidas de demora también sirve de disuasión.

— La ***respuesta*** abarca las acciones que se toman después de la detección y que evitan que un adversario tenga éxito o que mitigan las consecuencias graves posibles. Estas

acciones, las cuales suelen ser llevadas a cabo por el personal de seguridad, las fuerzas del orden u otros organismos gubernamentales, incluyen interrumpir y vencer al adversario mientras intenta retirar sin autorización o sabotear las fuentes para evitar que use la fuente para causar daño, recuperar las fuentes o, en su defecto, reducir la gravedad de las consecuencias. La posibilidad de una respuesta eficaz también puede servir como disuasión.

— La ***gestión de la seguridad física*** garantiza que se cuente con los recursos (de personal y financiamiento) para la seguridad física de las fuentes. También contempla la elaboración de procedimientos, políticas, registros y planes para la seguridad física de las fuentes y, en general, una cultura de la seguridad física más eficaz. Además, esta función incluye el desarrollo de procedimientos para el manejo adecuado de la información sensible y la protección en caso de que sea revelada sin autorización.

3.5. Diseño y evaluación de los sistemas de seguridad física

Un buen sistema de seguridad física debería integrar medidas que cumplan con las cinco funciones de seguridad, de manera que se asegure el blanco de cara a la amenaza, de acuerdo con los siguientes conceptos de seguridad:

La disuasión no se puede medir: El propósito de esta función es disuadir al adversario de cometer un acto doloso, por lo que el impacto de las medidas no es cuantificable. Por esto, el diseño de un sistema de seguridad física no se debería basar por completo en la disuasión.

Detección antes que demora: El propósito de la demora es dotar al personal de respuesta de suficiente tiempo para desplegar e interrumpir o anular los esfuerzos del adversario por cometer un acto doloso, por lo que la detección se debe dar antes que la demora. Si un adversario tiene suficiente tiempo para superar las barreras físicas y otros obstáculos antes de encontrarse con sensores de intrusión u otros dispositivos de detección, habrá completado las tareas más difíciles antes de ser detectado y podría sabotear o retirar

sin autorización la fuente radiactiva antes de que llegue el personal de respuesta. En este caso, las barreras, en lugar de cumplir la función de demorar, cumplen la de disuadir.

La detección requiere evaluación: La mayoría de medios de detección indican de manera indirecta que se está dando un posible acto doloso, como el acceso no autorizado o el retiro o sabotaje de una fuente radiactiva. El único método directo para identificar la causa es la observación que realice una persona, por lo que cuando se activa una alarma u otro indicador indirecto, siempre existen dudas al respecto. Por esta razón, para poder determinar la causa de la alarma, la detección siempre se debería complementar con la evaluación. Al evaluar las alarmas se requiere que una persona observe y emita un juicio al respecto; esto se logra mediante el despliegue del personal de respuesta para investigar la causa de la alarma o el uso de sistemas de circuito cerrado de televisión (CCTV) u otros sistemas similares. En ocasiones, los adversarios podrían intentar tomar ventaja de cualquier sistema de demora entre la detección y la evaluación para ocultar sus intenciones. Por eso, la meta de cualquier sistema de seguridad es la evaluación inmediata.

Demora mayor que la evaluación más el tiempo de respuesta: Un sistema de seguridad es exitoso si detecta y hace una correcta evaluación de un adversario que esté intentando cometer un acto doloso. Esto se tiene que dar en un plazo suficiente para que las medidas de demora resultantes permitan al personal de respuesta bloquear y detener al adversario antes de que se lleve a cabo el acto o ejecutar las acciones correctas para mitigar las consecuencias potencialmente graves. La relación entre la detección, la demora y la respuesta se conoce como *detección oportuna*.

Protección balanceada: Este es un concepto de funciones de seguridad equivalentes (disuasión, detección, demora, respuesta y gestión de la seguridad física) que proporcionan protección contra todas las amenazas en todas las rutas posibles. Es decir, los tiempos de demora en cada ruta, las medidas de detección asociadas a cada elemento de detección y las

respuestas resultantes proporcionan la protección necesaria para prevenir que un acto doloso tenga éxito.

Defensa en profundidad: Un concepto de varias capas y métodos de protección (estructural, técnica, de personal y de organización) que el adversario deberá superar o evadir para alcanzar su objetivo.

3.6. Integración de medidas de seguridad radiológica y física

Las medidas de seguridad radiológica y física comparten el objetivo de proteger la salud y la vida de las personas y el medio ambiente. Estas medidas deberán diseñarse e implementarse de manera integrada para que ninguna comprometa a la otra. Al poner en práctica las recomendaciones incluidas en esta publicación, los encargados del diseño de los sistemas de seguridad física deberán ponerse en contacto con expertos calificados en materia de seguridad radiológica para garantizar que no se ponga en peligro la seguridad de las personas o la protección del ambiente.

3.7. Enfoque graduado para la seguridad física

Los requisitos de seguridad física deben basarse en un enfoque graduado que tome en cuenta la evaluación de la amenaza actual, la atractividad relativa de la fuente radiactiva, la naturaleza de la fuente y las posibles consecuencias relacionadas con su retiro no autorizado o sabotaje. Este enfoque garantiza que las fuentes que podrían ocasionar las consecuencias más graves reciban el mayor nivel de protección.

3.8. Entender y abordar el entorno de amenaza

El diseño y la evaluación de un sistema de seguridad física deberían tomar en cuenta la evaluación actual de la amenaza interna y podría incluir la elaboración y la aplicación de una amenaza base de diseño (ver la sección Definiciones).

3.8.1. Evaluación de la amenaza nacional

El Código de Conducta establece que:

«Todo Estado debe definir su amenaza interna y evaluar su vulnerabilidad frente a dicha amenaza con respecto a las distintas fuentes utilizadas en su territorio con base en la posibilidad de una pérdida de control o un acto doloso que involucre una o varias fuentes radiactivas.» [NT]

Este proceso debe iniciar con una evaluación de la amenaza interna, la cual consiste en un análisis que documenta, a nivel nacional, las motivaciones, intenciones y capacidades creíbles de los posibles adversarios que podrían causar daño mediante el sabotaje de una instalación o el retiro no autorizado de una fuente radiactiva para propósitos dolosos. Normalmente, este proceso lo lleva a cabo una comunidad de inteligencia con información suministrada por los ministerios del interior, defensa, transporte y relaciones exteriores, la policía, personal de aduanas y guardia costera, así como otros organismos cuyas responsabilidades estén relacionadas con la seguridad. También podría estar involucrada la autoridad reguladora, pero, de no ser así, los organismos nacionales pertinentes le deberían hacer llegar la evaluación de la amenaza actual para la elaboración de su programa regulatorio en materia de seguridad física de fuentes radiactivas.

El proceso de evaluación es de razonamiento deductivo. A partir de lo que se sabe, se emite un juicio sobre cómo se podrían comportar los adversarios o los grupos de adversarios en el futuro. Esto incluye, por ejemplo, sucesos pasados y las capacidades que se conocen de los adversarios para atacar los diferentes tipos de instalaciones donde se almacenan o usan las fuentes radiactivas. La evaluación de la amenaza deberá cubrir al menos los siguientes atributos o características para cada adversario interno y externo que se identifique:

— *Motivación*: Política, económica, ideológica o personal.

— *Grado de compromiso*: Desinterés por la salud, la seguridad, el bienestar o la supervivencia propia.

[NT] Notal del traductor: Definición tomada del *Código de conducta*

— *Intenciones*: Sabotaje del material o la instalación (retiro no autorizado), pánico y perturbación en la población, desestabilidad política, lesiones y muertes masivas.

— *Tamaño del grupo*: Fuerza de ataque, coordinación y apoyo.

— *Armas*: Tipo, número, disponibilidad y grado de improvisación de las mismas.

— *Herramientas*: Equipo mecánico, térmico, manual, de energía, electrónico, electromagnético y de comunicaciones.

— *Medios de transporte*: Público, privado, marítimo, terrestre, aéreo, tipo, número y disponibilidad.

— *Capacidades técnicas*: ingeniería, uso de explosivos y químicos, comunicación y experiencia paramilitar.

— *Habilidades informáticas*: Uso de computadoras y sistemas de control automático como apoyo directo en caso de ataques físicos, espionaje, ataques a equipos de cómputo, recaudación de dinero, etc.

— *Conocimiento*: Objetivos, planes y procedimientos de la instalación, medidas de seguridad, procedimientos de seguridad radiológica y de protección contra la radiación, operaciones, posible uso de material nuclear o radiactivo.

— *Financiamiento*: Origen, monto y disponibilidad.

— *Agentes internos*: Conspiración, pasivos o activos, violentos o no violentos y número de agentes.

— *Estructura de apoyo*: Simpatizantes locales, apoyo organizacional y logística.

— *Tácticas*: Visibles y encubiertas.

Una vez que el Estado haya hecho la evaluación de su amenaza, deberá definir la base sobre la cual establecer los reglamentos para la seguridad de las fuentes radiactivas. Un posible enfoque que se puede adoptar es elaborar regulaciones con base en la evaluación de la amenaza interna; otro es elaborarlas con base en la amenaza base de diseño (ver más

adelante), para la cual la evaluación de la amenaza interna se convierte en una entrada más de información. Al elegir la base regulatoria, el Estado debe considerar diversos factores, incluida la gravedad de las consecuencias asociadas con los actos dolosos que involucren fuentes radiactivas que existan en el Estado, su capacidad para establecer sistemas de protección eficaces que usen cada uno de los enfoques y la habilidad de la autoridad reguladora para implementar los diferentes enfoques.

Es importante resaltar que no todos los Estados requieren el uso de la amenaza base de diseño como enfoque para su sistema regulatorio. Sin embargo, si no se elige este enfoque, el Estado siempre deberá preparar una evaluación de la amenaza nacional y mantenerla vigente.

3.8.2. Amenaza base de diseño

Una amenaza base de diseño, definida a nivel nacional, es una herramienta que sirve para establecer requisitos de desempeño en el diseño de sistemas de protección física para tipos específicos de instalaciones. También ayuda a los operadores y las autoridades del Estado a evaluar la eficacia de los sistemas para enfrentar a los adversarios mediante la medición del desempeño de los sistemas de seguridad física frente a las capacidades del adversario descritas en la amenaza base de diseño, para lo cual se realizan pruebas de vulnerabilidad. La amenaza base de diseño es una descripción detallada de las motivaciones, intenciones y capacidades de los posibles adversarios contra los cuales se diseñaron y evaluaron los sistemas de protección. Las capacidades del adversario, interno o externo, ayudan a determinar los requisitos de detección, demora y respuesta para que un sistema de seguridad física sea eficaz ante una amenaza base de diseño.

El desarrollo de una amenaza base de diseño será diferente para cada Estado debido a las diferencias sociales, culturales y geopolíticas. Al igual que con la evaluación de la amenaza interna, la elaboración de una amenaza base de diseño requiere del esfuerzo

conjunto de las autoridades nacionales, tales como los organismos de inteligencia y de seguridad, las fuerzas del orden, las autoridades reguladoras y los operadores. Una amenaza base de diseño se puede revisar cada cierto tiempo a la luz de la nueva información que proporcionen los organismos del Estado. Se puede encontrar más información sobre el proceso de la amenaza base de diseño en la Ref. [13].

3.8.3. Amenazas internas

Al diseñar sistemas de seguridad física, se le debería prestar especial atención a las amenazas internas, las cuales podrían provenir de una o más personas con acceso autorizado a una instalación y un conocimiento profundo de las actividades o ubicaciones de la fuente. Pueden ser empleados o contratistas que tengan la posibilidad de retirar las fuentes o robar información con el propósito de cometer actos dolosos o sabotear el lugar. Además, estas personas podrían buscar trabajo en una instalación con el objetivo de cometer actos dolosos, ayudar a adversarios externos a retirar las fuentes radiactivas, o bien, llevar a cabo actos hostiles. Las amenazas internas y las contramedidas adecuadas y recomendadas se explican con más detalle en la Ref. [15].

3.8.4. Amenaza aumentada

Un sistema de seguridad física debería contrarrestar eficazmente la amenaza evaluada actualmente. Sin embargo, deberían existir disposiciones que garanticen que el nivel de seguridad pueda aumentar cuando la amenaza sea mayor. Estas deberían incluir medidas de seguridad adicionales o limitar el acceso a las fuentes radiactivas.

3.9. Prueba de vulnerabilidad

Una prueba de vulnerabilidad, también conocida como encuesta de seguridad o prueba de seguridad, consiste en un método para evaluar los sistemas de seguridad física. Es una evaluación sistemática de la eficacia del sistema de seguridad física en términos de la protección que brinda frente a una amenaza evaluada (o una amenaza base de diseño, si

existiera). La prueba de vulnerabilidad puede ser de carácter general o específico, ser realizada localmente por el operador, el Estado o la autoridad reguladora y puede servir para la elaboración de reglamentos por parte del Estado o para demostrar que el operador cumple con los reglamentos. En el Apéndice III se puede encontrar más información sobre cómo realizar una prueba de vulnerabilidad.

4. Establecimiento de un programa regulatorio para la seguridad física de las fuentes radiactivas

Las disposiciones del Código de Conducta relacionadas con la seguridad física de las fuentes radiactivas fueron fortalecidas para brindar medidas que reduzcan la posibilidad de actos dolosos. El Código también menciona específicamente que los Estados deberían brindar la debida atención a las fuentes radiactivas que se considere tengan el potencial de provocar consecuencias inaceptables si se utilizaran en actos dolosos. En tales situaciones, el OIEA establece requisitos y ofrece recomendaciones para la preparación y respuesta ante emergencias, e intervención y remediación de zonas contaminadas [5, 9, 10]. La Comisión Internacional de Protección Radiológica [11] brinda recomendaciones sobre cómo proteger a las personas de la radiación después de un ataque radiológico.

Tales actos maliciosos y sus posibles consecuencias incluyen:

— la colocación deliberada de una fuente rota o sin blindaje en una zona pública

— la dispersión deliberada de material radiactivo con la intención de causar efectos negativos en la salud (por ejemplo, mediante el uso de un dispositivo de dispersión radiológica (DDR)

— el uso de un DDR con el propósito de contaminar suelos, edificios e infraestructura lo cual puede llevar a impedir el acceso a esas zonas, lo cual se puede basar en criterios de protección radiológica, de impacto económico y de costo de limpieza y reconstrucción

Varios Estados ya tienen un programa regulatorio que cubre actividades como la autorización, revisión, evaluación, inspección y verificación del cumplimiento [16]. Esta sección brinda a las autoridades reguladoras recomendaciones sobre cómo elaborar o mejorar los programas regulatorios que aborden la seguridad de las fuentes radiactivas y así reducir la posibilidad de que se presenten actos dolosos que involucren a dichas fuentes. Las medidas de seguridad radiológica y física deberían diseñarse e implementarse de manera integrada para que una no comprometa a la otra.

El establecimiento de un programa regulatorio para la seguridad física de las fuentes radiactivas requiere que la autoridad reguladora siga tres pasos básicos:

— **Paso 1**: Establecer niveles graduados de seguridad física con metas y objetivos correspondientes a cada nivel de seguridad (ver Sección 4.1).

— **Paso 2**: Determinar el nivel de seguridad física aplicable a una fuente radiactiva en particular (ver Sección 4.2).

— **Paso 3**: Elegir e implementar un enfoque regulatorio (prescriptivo, basado en el desempeño o combinado) para indicar a los operadores cómo diseñar, implementar y evaluar las medidas de seguridad física y cumplir con los objetivos de seguridad física del Cuadro 1 (ver Sección 4.3).

4.1. Paso 1: Establecer niveles graduados de seguridad física con metas y los objetivos correspondientes

Las fuentes radiactivas tienen una gran variedad de características (entre ellas, la actividad) que las hacen atractivas en varios niveles para los adversarios. Se deberían usar medidas de seguridad física pertinentes y eficaces para garantizar que las fuentes estén debidamente protegidas al usar un enfoque graduado. Para poder garantizar una capacidad adecuada de protección sin imponer medidas demasiado restrictivas, se debería usar el concepto de niveles de seguridad. Se han definido tres niveles de seguridad física (A, B y C)

para especificar de manera gradual el desempeño que debe cumplir un sistema de seguridad física. El nivel de seguridad A requiere el grado más alto de protección, mientras que los otros niveles requieren niveles progresivamente menores.

A cada nivel de seguridad le corresponde una meta, la cual define el resultado general que debería alcanzar el sistema de seguridad física para un nivel de seguridad determinado. Se han definido las siguientes metas:

— **Nivel de seguridad A**: *Prevenir* el retiro no autorizado de una fuente.

— **Nivel de seguridad B**: *Minimizar la posibilidad* de un retiro no autorizado de una fuente.

— **Nivel de seguridad C**: *Reducir la posibilidad* de un retiro no autorizado de una fuente.

Los actos dolosos pueden incluir el retiro no autorizado o sabotaje de una fuente. Si bien las metas de seguridad solo abordan el retiro no autorizado, su cumplimiento reducirá la posibilidad de que se consume un acto de sabotaje. Los sistemas de seguridad que cumplan con las metas indicadas anteriormente proporcionarán cierta capacidad (si bien limitada) para detectar y responder a un acto de sabotaje.

Para poder cumplir las *metas*, es necesario alcanzar un nivel de desempeño adecuado en cada una de las *funciones* de seguridad: disuasión, detección, demora, respuesta y gestión de la seguridad física. Tal nivel de desempeño se define como un grupo de *objetivos* para cada una de las funciones, los cuales establecen el resultado que se desea obtener al combinar las *medidas* aplicadas a cada objetivo. La disuasión es una función de seguridad que es difícil calcular. Por ello, en este documento no se le ha asignado un grupo de objetivos y medidas de seguridad.

Los niveles de seguridad física y los objetivos asociados se resumen en el Cuadro 2.

Cuando un objetivo se repite en dos o más niveles de seguridad, se espera que se cumpla de manera más estricta en los niveles de seguridad más altos.

4.2. Paso 2: Determinar el nivel de seguridad aplicable a una fuente en particular

Para especificar el nivel de seguridad adecuado de una fuente, se debe considerar el posible daño que esta podría causar si se utilizara en un acto doloso, pues este servirá de guía para asignar el nivel de seguridad apropiado. El proceso sigue los siguientes pasos:

— Categorizar las fuentes con base en su potencial para causar daños si se usaran con propósitos dolosos (incluida la agrupación de fuentes en una ubicación determinada, según proceda) (ver Sección 4.2.1).

— Asignar un nivel de seguridad adecuado a cada categoría (ver Sección 4.2.2).

4.2.1. Clasificación de las fuentes radiactivas

El Código de Conducta se aplica a fuentes radiactivas que representen un riesgo importante para las personas, la sociedad y el medio ambiente, es decir, a las fuentes en categorías de la 1 a la 3. Se deberían aplicar las medidas de seguridad apropiadas para reducir la posibilidad de actos dolosos que involucren.

La clasificación de las fuentes utilizada en el Código de Conducta se basa en el concepto de «fuentes peligrosas», las cuales se calculan en términos de valores D [17]. Este concepto se explica con más detalle en el documento del OIEA titulado *Clasificación de las fuentes radiactivas* [3]. Esta guía recomienda emplear un sistema de clasificación para las fuentes, particularmente las usadas en el comercio, la medicina, la agricultura, la investigación y la educación. Este sistema de clasificación también se podría aplicar en el ámbito nacional, según corresponda, a las fuentes en programas militares o de defensa. Este sistema brinda una base armonizada internacionalmente para la toma de decisiones informadas sobre el riesgo y se basa en un método lógico y transparente que brinda flexibilidad para aplicarse en circunstancias diversas. La toma de decisiones informadas sobre el riesgo se pueden realizar con un enfoque graduado del control regulatorio de las fuentes radiactivas para propósitos de seguridad radiológica y física.

Cuadro 2. Niveles y objetivos de seguridad

Funciones de la seguridad física	Objetivos de seguridad física		
	Meta del Nivel de seguridad A: Prevenir el retiro no autorizado [a]	Meta del Nivel de seguridad B: Minimizar la posibilidad de un retiro no autorizado [a]	Meta del Nivel de seguridad C: Reducir la posibilidad de un retiro no autorizado [a]
Detección	Detectar inmediatamente todo acceso no autorizado al área o ubicación segura de la fuente		
	Detectar inmediatamente todo intento de retiro no autorizado de la fuente, incluido el de un interno	Detectar todo intento de retiro no autorizado de la fuente	Detectar el retiro no autorizado de la fuente
	Evaluar inmediatamente la detección		
	Comunicarlo inmediatamente al personal de respuesta		
	Proporcionar los medios para detectar la pérdida de una fuente mediante la verificación		
Demora	Crear suficiente demora después de la detección para que el personal de respuesta interrumpa el retiro no autorizado	Crear demora para minimizar la posibilidad de un retiro no autorizado	Crear demora para reducir la posibilidad de un retiro no autorizado
Respuesta	Responder inmediatamente a una alarma evaluada con suficientes recursos para	Iniciar inmediatamente la respuesta para interrumpir el retiro no autorizado	Poner en práctica acciones adecuadas en caso de un retiro no autorizado de una fuente

	interrumpir y prevenir el retiro no autorizado		
Gestión de la seguridad física	Instalar controles que restrinjan el acceso a la ubicación de la fuente únicamente a personas autorizadas		
	Garantizar la probidad de las personas autorizadas		
	Identificar y proteger la información sensible		
	Proporcionar un plan de seguridad física		
	Garantizar la capacidad para lidiar con eventos de seguridad física incluidos en el plan de contingencia (ver Definiciones)		
	Establecer un sistema de reporte de eventos de seguridad		

[a] Cumplir con estas metas también reducirá la posibilidad de que un acto de sabotaje tenga éxito.

Reconociendo que la salud humana es de suma importancia, el sistema de clasificación se basa principalmente en el potencial que tengan las fuentes para causar efectos deterministas sobre la salud. El valor D es la actividad específica del radionucleido de una fuente, la cual, si no se tiene bajo control, podría causar efectos deterministas graves en una amplia variedad escenarios, entre ellos, una exposición externa procedente de una fuente no blindada y la exposición interna a raíz de la dispersión (mediante fuego o explosión) del material de la fuente (NT: *Clasificación de las fuentes radiactivas* 5).

La actividad del material radiactivo (A) de las fuentes varía en orden de magnitud. Los valores D se usan para normalizar las distintas actividades a fin de ofrecer un punto de referencia al comparar los riesgos. Esto se debería hacer tomando la actividad de la fuente

(en TBq) y dividiéndola entre el valor D del radionucleido correspondiente (NT: *Clasificación de las fuentes radiactivas* 9).

Cabe señalar que existe la posibilidad de que una cantidad inferior a los valores D sea peligrosa [17]. Este puede ser el caso de que se administre una fuente radiactiva a una persona con fines dolosos.

En el Cuadro 3 se expone el umbral de actividades para los radionucleidos del Código de Conducta que aplican en fuentes de categorías de la 1 a la 3. Para los radionucleidos que no están en este cuadro, ver las Ref. [3, 17].

«En algunas situaciones podrá ser adecuado asignar una categoría a una fuente basándose únicamente en A/D, por ejemplo, cuando no se conoce o no se ha confirmado la práctica para la que se puede utilizar la fuente. En cambio, cuando se conocen las circunstancias de utilización de la fuente, la autoridad reguladora puede decidir que es oportuno modificar esa categoría asignada utilizando otra información sobre la fuente o su utilización. En algunas circunstancias puede ser conveniente asignar una categoría basándose en la práctica en la que se utiliza la fuente» (NT: *Clasificación de las fuentes radiactivas* 9) (ver Cuadro 4).

El sistema de clasificación tiene cinco categorías, como se muestra en el Cuadro 4, las cuales deberían ser suficientes «para poder aplicarlo en la práctica, sin precisiones innecesarias. Dentro de este sistema, se considera que las fuentes de la categoría 1 son las más “peligrosas” porque pueden suponer un riesgo altísimo para la salud de los seres humanos si no se manejan en condiciones de seguridad [radiológica] y física. La exposición durante solo unos cuantos minutos a una fuente de categoría 1 no blindada puede ser fatal. En el extremo inferior del sistema de clasificación, las fuentes de la categoría 5 son las menos peligrosas; ahora bien, incluso ellas pueden dar lugar a dosis superiores a las dosis límite si no se controlan correctamente y, por consiguiente, hay que mantenerlas bajo el adecuado

control regulador No conviene subdividir las categorías porque se alcanzaría un grado de precisión innecesario y se menoscabaría la armonización internacional» (NT: *Clasificación de las fuentes radiactivas* 6).

4.2.1.1. Fuentes radiactivas no listadas

Para las fuentes que no están incluidas en el Cuadro 4, la autoridad reguladora les podría asignar una categoría con base en la proporción A/D.

4.2.1.2. Radionucleidos de vida media breve

«En algunas prácticas, como la medicina nuclear, se utilizan radionucleidos que tienen una vida media breve en una forma de fuente que no está sellada. Entre los ejemplos de esas aplicaciones está el radionucleido Tc^{99m} en radiodiagnósticos y el I^{131} en radioterapia. En esas situaciones, se pueden aplicar los principios del sistema de clasificación en categorías para determinar una categoría para la fuente… Estas situaciones deberían ser examinadas una por una» (NT: *Clasificación de las fuentes radiactivas* 9).

4.2.1.3. Fuentes radiactivas no selladas

La autoridad reguladora podría asignar una categoría a una fuente no sellada con base en la proporción A/D.

4.2.1.4. Desintegración radiactiva

Si la actividad de una fuente se desintegra a un nivel inferior al umbral adecuado que se indica en el Cuadro 3 o al que normalmente se utiliza (como se muestra en el Cuadro 4), la autoridad reguladora podría permitir al operador clasificar de nuevo la fuente con base en la proporción A/D.

4.2.1.5. Suma de las fuentes [NT]

Habrá situaciones en las que las fuentes radiactivas estén muy próximas unas a otras, como en los procesos de fabricación (por ejemplo, en la misma habitación o el mismo edificio) o en instalaciones de almacenamiento (por ejemplo, en el mismo recinto). En tales

[NT] Sección adaptada de Clasificación de las fuentes radiactivas, pág. 9-10.

circunstancias, la autoridad reguladora podría optar por sumar la actividad de las fuentes para determinar una clasificación en categorías específicas de la situación a efectos de aplicar medidas de control regulador. En esas situaciones, habría que dividir la actividad sumada del radionucleido por el valor D adecuado y comparar la proporción A/D calculada con las proporciones A/D dadas en el cuadro 2, gracias a lo cual se podría clasificar por categorías el conjunto de las fuentes basándose en la actividad. Si se suman fuentes con diversos radionucleidos, habría que utilizar la suma de las proporciones A/D para determinar la categoría, de conformidad con la fórmula:

$$\text{Suma de A/D} = \sum_n \frac{\sum_i A_{i,n}}{D_n}$$

En que:

$A_{i,n}$ = actividad de cada fuente *i* del radionucleido *n*.

D_n = valor D para el radionucleido *n*.

Se puede encontrar más información sobre la suma de fuentes radiactivas en la Ref. [3].

4.2.2. Asignación de niveles de seguridad

Como condición base, la autoridad reguladora podría usar las categorías indicadas anteriormente para asignarle a una fuente en particular su nivel de seguridad física.

Las fuentes de la Categoría 1 deberían contar con medidas de seguridad física que cumplan con los objetivos de seguridad del Nivel de seguridad A. Las fuentes de la Categoría 2 deberían contar con medidas que cumplan los objetivos de seguridad del Nivel de seguridad B. Las fuentes de la Categoría 3 deberían contar con medidas que cumplan los objetivos de seguridad del Nivel de seguridad C.

Las Normas básicas internacionales de seguridad para la protección contra la radiación ionizante y para la seguridad de las fuentes de radiación (párrafo 2.34 [5]) indican requisitos

generales para la seguridad de las fuentes radiactivas. En esta publicación se considera que si bien esas medidas de control brindan suficiente protección a las fuentes en las categorías 4 y 5, a las fuentes en categorías 1, 2 y 3 se les deberían aplicar medidas más estrictas como las especificadas en este documento para reducir la posibilidad de que ocurran actos dolosos que involucren a dichas fuentes. Además, tomando en cuenta la amenaza nacional, la autoridad reguladora podría decidir fortalecer las medidas de seguridad para las fuentes en las categorías 4 y 5 en circunstancias pertinentes. En el Cuadro 5 se encuentra un resumen de este enfoque.

Si bien este enfoque se puede ver como la condición base, un acto doloso podría no necesariamente involucrar a las fuentes de niveles más altos según esta clasificación. Por ejemplo, la mayoría de fuentes de la Categoría 1 están blindadas y dentro de dispositivos o instalaciones fijas. Retirar tales fuentes podría tomar tiempo y exponer a los adversarios a un nivel de radiación bastante perjudicial. Por tal motivo, es posible que los adversarios se centren en fuentes de categorías más bajas, más accesibles, de manipulación menos riesgosa, portables y menos ocultas.

El propósito de clasificar las fuentes radiactivas es proporcionar una base internacionalmente aceptada para la toma de decisiones basadas en el riesgo, incluidas las medidas para reducir la posibilidad de un acto doloso. No obstante, las consecuencias socioeconómicas de tales actos fueron excluidas de los criterios de clasificación puesto que no existe una metodología para calcular y comparar estas consecuencias, especialmente en el ámbito internacional.

Cuadro 3. Actividades correspondientes al umbral de categorías [NT]

Radionucleido	Categoría 1 1000 xD		Categoría 2 10 xD		Categoría 3 D	
	(TBq)	(Ci)[a]	(TBq)	(Ci)[a]	(TBq)	(Ci)[a]
Am-241	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Am-241/Be	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+(X)
Cf-252	2.E+01	5.E+02	2.E-01	5.E-(X)	2.E-02	5.E-01
Cm-244	5.E+01	1.E+03	5.E-01	1.E+01	5.E-02	1.E+00
Co-60	3.E+01	8.E+02	3.E-01	8.E+00	3.E-02	8.E-01
Cs-137	1.E+02	3.E+03	1.E+00	3.E+01	1.E-01	3.E+(X)
Gd-153	1.E+03	3.E+04	1.E+01	3.E+02	1.E+00	3.E+01
Ir-192	8.E+01	2.E+03	8.E-01	2.E+01	8.E-02	2.E+(X)
Pm-147	4.E+04	1.E+06	4.E+02	1.E+04	4.E+01	1.E+03
Pu-238	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Pu-239[b]/Be	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+(X)
Ra-226	4.E+01	1.E+03	4.E-01	1.E+01	4.E-02	1.E+(X)
Se-75	2.E+02	5.E+03	2.E+00	5.E+01	2.E-01	5.E+00
Sr-90 (Y-90)	1.E+03	3.E+04	1.E+01	3.E+02	1.E+00	3.E+01
Tm-170	2.E+04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02
Yb-169	3.E+02	8.E+03	3.E+00	8.E+01	3.E-01	8.E+(X)
Au-198*	2.E+02	5.E+03	2.E+00	5.E+01	2.E-01	5.E+(X)
Cd-109*	2.E+04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02
Co-57*	7.E+02	2.E+04	7.E+00	2.E+02	7.E-01	2.E+01
Fe-55*	8.E+05	2.E+07	8.E+03	2.E+05	8.E+02	2.E+04
Ge-68*	7.E+02	2.E+04	7.E+00	2.E+02	7.E-01	2.E+01
Ni-63*	6.E+04	2.E+06	6.E+02	2.E+04	6.E+01	2.E+03
Pd-103*	9.E+04	2.E+06	9.E+02	2.E+04	9.E+01	2.E+03
Po-210*	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+(X)
Ru-106 (Rh-106)*	3.E+02	8.E+03	3.E+00	8.E+01	3.E-01	8.E+00
Tl-204*	2.E+04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02

[a] «Los valores principales que se deben usar figuran en TBq. Se dan los valores en curios por su utilidad práctica y se redondean después de haberlos convertido» (NT: *Clasificación de las fuentes radiactivas* 48).

[b] «Para los múltiplos de D habrá que tener en cuenta diversas cuestiones atinentes a la criticalidad y las salvaguardias» (NT: *Clasificación de las fuentes radiactivas* 48).

* Es muy poco probable que estos radionucleidos se usen en fuentes radiactivas individuales con niveles de actividad que los sitúen en las categorías 1, 2 o 3; por lo tanto, no estarían sujetos a los párrafos del Código relacionados con los registros nacionales o los controles de importación y exportación.

[NT] Cuadro tomado del documento titulado *Clasificación de las fuentes radiactivas, pág. 47*.

Cuadro 4. Categorías para las fuentes utilizadas en actividades comunes [NT]

Categoría	Fuente [a]	A/D [b]
1	Generadores termoeléctricos de radioisótopos (RTGs) Irradiadores Fuentes de teleterapia Fuentes de teleterapia fija de haces múltiples (cuchillo gamma)	A/D ≥ 1000
2	Fuentes de radiografía gamma industrial Fuentes de braquiterapia de elevada/media tasa de dosis	1000 > A/D ≥ 10
3	Calibradores industriales fijos con fuentes de actividad alta [c] Calibradores para diagrafía de pozos	10 > A/D ≥ 1
4	Fuentes de braquiterapia de baja tasa de dosis (salvo placas oculares e implantes permanentes) Calibradores industriales sin fuentes de actividad alta Densitómetros de huesos Eliminadores de estática	1 > A/D ≥ 0.01
5	Fuentes de braquiterapia de baja tasa de dosis, placas oculares e implantes permanentes Aparatos de análisis mediante fluorescencia por rayos X (FRX) Aparatos detectores por captura de electrones Fuentes de espectrometría Mössbauer Fuentes de examen mediante tomografía por emisión de positrones (TEP)	0.01 > A/D y A > exim. [d]

[a] Se ha tomado en consideración otros factores más que solo la proporción A/D al asignar la categoría a las fuentes (ver la Ref. [3] Anexo I).

[b] «Se puede utilizar esta columna para determinar la categoría de una fuente basándose únicamente en la proporción A/D, método que puede ser adecuado, por ejemplo, si no se conoce la práctica o no figura en la lista; si las fuentes tienen una vida media breve y/o no están selladas, o bien si se han sumado las fuentes (ver la Ref. [3], párrafo 3.5)»

[c] En la Ref. [3], Anexo I, se dan ejemplos.

[d] Las cantidades eximidas figuran en la Lista I de la Ref. [5].

[NT] Cuadro y notas al pie tomadas del documento titulado *Clasificación de las fuentes radiactivas, pág. 7*.

4.2.3. Consideraciones adicionales para la asignación de niveles de seguridad

El Anexo 1 del Código de Conducta menciona que los Estados deberían brindar la debida atención a las fuentes que consideren que tienen el potencial de causar consecuencias inaceptables si se utilizaran en actos dolosos.

Aunque las Ref. [3, 17] toman en cuenta algunos de los factores indicados más adelante, la autoridad reguladora debe poner especial atención a estos factores y consideraciones al asignar niveles de seguridad a las fuentes radiactivas. Estos factores representan variables que son específicas para cada fuente, así como su uso y su ubicación; además, pueden afectar el nivel de seguridad adecuado para una fuente o instalación en particular.

4.2.3.1. Atractividad de la fuente

Además de la actividad, existen otros factores que pueden hacer que las fuentes sean más atractivas para su uso en actos dolosos. Entre ellos, están los siguientes:

— La forma química y física del material radiactivo de la fuente, las cuales podrían hacerla fácilmente dispersable y, por lo tanto, más atractiva para un adversario.

— La naturaleza de la emisión radiactiva. Algunos radionucleidos producen dosis más altas por unidad consumida, especialmente los emisores alfa. Las fuentes que contengan estos radionucleidos pueden ser más atractivas para su uso en dispositivos de dispersión radiológica (DDR).

— Fácil manejo. Las fuentes que se pueden ser manejadas fácilmente o que son de fácil acceso pueden ser más atractivas puesto que la fuente se puede mover fácilmente y es menos probable que el adversario reciba una dosis alta de radiación. Un ejemplo de esto es una fuente que esté dentro de un dispositivo portátil autoblindado.

— Co-ubicación. Varias fuentes o grandes cantidades de material radiactivo co-ubicados pueden ser atractivos para un adversario puesto que si logra atravesar el sistema de seguridad

física con éxito, podría retirar o sabotear suficiente material para provocar consecuencias muy graves.

— Valor económico percibido de la fuente o del equipo dentro del cual se encuentre.

La autoridad reguladora podría tomar en cuenta la atractividad de las fuentes al determinar el nivel de seguridad asignado y las medidas de seguridad que se apliquen a ese nivel.

4.2.3.2. Fuentes en almacenamiento

Las fuentes radiactivas en almacenamiento deberían ser protegidas según las medidas indicadas en este documento y la clasificación y el nivel de seguridad física que apliquen para tal fuente.

4.2.3.3. Vulnerabilidad y nivel de amenaza

El nivel de amenaza interna y cualquier aumento en este nivel podrían justificar una evaluación del nivel de seguridad física asignado a una fuente; para esto, se toma en cuenta cualquier otro atributo de la fuente (por ejemplo, la atractividad o vulnerabilidad). De manera alternativa, se podrían fortalecer las medidas específicas para el nivel de seguridad física de una fuente en particular.

4.2.3.4. Fuentes móviles, portátiles y remotas

Las fuentes utilizadas en aplicaciones de campo (por ejemplo, radiografía y diagrafía de pozos) están contenidas en dispositivos diseñados para que sean portátiles y son transportadas frecuentemente a diferentes lugares de trabajo. La facilidad de manejo y su presencia en vehículos que están fuera de instalaciones protegidas hacen que sean atractivas para un retiro no autorizado.

Cuadro 5. Niveles de seguridad física estándar para fuentes de uso común [NT]

Categoría	Fuente	A/D	Nivel de seguridad
1	RTGs Irradiadores Fuentes de teleterapia Fuentes de teleterapia fija de haces múltiples (cuchillo gamma)	A/D ≥ 1000	A
2	Fuentes de radiografía gamma industrial Fuentes de braquiterapia de tasa de dosis elevada o media	1000 > A/D ≥ 10	B
3	Calibradores industriales fijos con fuentes de actividad alta Calibradores para diagrafía de pozos	10 > A/D ≥ 1	C
4	Fuentes de braquiterapia de baja tasa de dosis (salvo placas oculares e implantes permanentes) Calibradores industriales sin fuentes de actividad alta Densitómetros de huesos Eliminadores de estática	1 > A/D ≥ 0.01	Aplicar las medidas descritas en las Normas básicas de seguridad [5]
5	Fuentes de braquiterapia de baja tasa de dosis, placas oculares e implantes permanentes Aparatos de análisis mediante fluorescencia por rayos X (FRX) Aparatos detectores por captura de electrones Fuentes de espectrometría Mössbauer Fuentes de examen mediante tomografía por emisión de positrones (TEP)	0.01 > A/D y A > exim.	

Al reconocer que las medidas de seguridad de las fuentes fijas no son aplicables a las que se utilizan en trabajos de campo, se deberían aplicar medidas alternativas para cumplir con el objetivo de seguridad. Referirse a las medidas de detección y demora para los niveles

[NT] Cuadro tomado del documento *Clasificación de las fuentes radiactivas,* pág. 7.

de seguridad B y C (Sección 4.3.1), así como a las medidas de seguridad física ilustrativas para fuentes móviles que se encuentran en el Apéndice IV.

Las fuentes que se utilizan en ubicaciones remotas podrían ser retiradas por personal no autorizado y transportadas fuera del área segura antes de que sea posible una respuesta eficaz.

La autoridad reguladora podría tomar en cuenta la movilidad, la portabilidad y la ubicación de la fuente a la hora de asignar el nivel de seguridad de una fuente, así como añadir medidas dentro del nivel de seguridad asignado para compensar estas condiciones.

4.3. Paso 3: Elegir e implementar un enfoque reglamentario

Existen tres enfoques diferentes que podría utilizar la autoridad reguladora para indicar a los operadores la manera de demostrar que cumplen los objetivos de seguridad física especificados en el Cuadro 2. Los enfoques elegidos por la autoridad reguladora deberían tomar en cuenta sus propias capacidades y recursos, las capacidades y los recursos de los operadores que regula y las diferentes fuentes que deben protegerse:

— El *enfoque prescriptivo* establece medidas de seguridad específicas determinadas por la autoridad reguladora para cumplir con los objetivos de seguridad física en cada nivel de seguridad física. En esta sección se identifica un grupo de medidas de este tipo para cada nivel de seguridad, las cuales podrían ser adoptadas por la autoridad reguladora como requisitos en ausencia de una amenaza base de diseño. De manera alternativa, la autoridad reguladora podría usar las medidas de seguridad física presentadas en esta publicación como punto de partida para después ajustarlas a las circunstancias nacionales. El uso del enfoque prescriptivo es particularmente adecuado cuando la combinación de la amenaza y las posibles consecuencias es baja o cuando no es posible realizar una evaluación detallada de la amenaza. El enfoque prescriptivo tiene la ventaja de que su implementación es simple para la autoridad reguladora y los operadores, además de ser fácil de inspeccionar y auditar. La

desventaja es su relativa falta de flexibilidad a la hora de abordar circunstancias reales. Por ejemplo, la experiencia ha demostrado que un operador puede cumplir con las medidas prescritas pero no cumplir el propósito del sistema de seguridad física de proteger los blancos de una amenaza real o definida. Como resultado, cuando se utiliza este enfoque, la autoridad reguladora debe garantizar que se realicen inspecciones o pruebas de seguridad para evaluar la eficacia general del sistema de seguridad física de la instalación en el cumplimiento de la meta de seguridad y los objetivos para el nivel de seguridad física aplicable (ver Sección 4.3.1).

— El *enfoque basado en el desempeño* es uno donde la autoridad reguladora ofrece flexibilidad al operador para proponer una combinación particular de medidas de seguridad física que se utilizarán para cumplir con los objetivos de seguridad física del Cuadro 2. Las medidas propuestas deberían basarse en la prueba de vulnerabilidad y la información proporcionada por la autoridad reguladora, que a su vez se basa en la evaluación de la amenaza nacional y, cuando sea pertinente, la amenaza base de diseño. Las ventajas de este enfoque son el reconocer que un sistema de seguridad física eficaz puede estar compuesto por distintas combinaciones de medidas y que las circunstancias de cada operador son diferentes. Como prerrequisito, este enfoque requiere que el operador y la autoridad reguladora sean relativamente expertos en la materia (ver Sección 4.3.2).

— Un *enfoque combinado* cuenta con elementos tanto del enfoque prescriptivo como del basado en el desempeño, y es posible obtener diferentes versiones. Por ejemplo, la autoridad reguladora puede adoptar un grupo de medidas de seguridad y permitirle al operador elegir cuáles usar, a la vez que le exige demostrar que el sistema de seguridad física en general cumple con los objetivos de seguridad aplicables. Otra opción es que la autoridad reguladora use un enfoque basado en el desempeño para las fuentes que de utilizarse en actos dolosos, puedan causar consecuencias más graves y un enfoque prescriptivo para las fuentes que puedan causar consecuencias menos severas. También, en situaciones particulares, los

requisitos prescriptivos podrían complementarse con requisitos enfocados en el desempeño. La principal ventaja del enfoque combinado es su flexibilidad (ver Sección 4.3.3).

El resto de esta sección brinda a las autoridades reguladoras guías sobre el uso de cada enfoque.

4.3.1. Enfoque prescriptivo

La autoridad reguladora podría especificar las medidas de seguridad que los operadores están obligados a poner en práctica para cumplir con los objetivos de seguridad física del Cuadro 2. Los Cuadros 6, 7 y 8 indican las medidas que buscan cumplir con los objetivos de los niveles A, B y C, respectivamente. Estos cuadros incluyen medidas de seguridad física para fuentes en uso o en almacenamiento, las cuales se explican con más detalle después de cada cuadro y podrían variar dependiendo de si la fuente está en uso o almacenamiento, o si es móvil o portátil. En el Apéndice I se puede encontrar más información sobre estas medidas. En el Apéndice IV se proporcionan medidas de seguridad física ilustrativas que se podrían aplicar a instalaciones y actividades en particular.

Introducción a las medidas de seguridad para el Nivel A

La meta del Nivel de seguridad A es **prevenir el retiro no autorizado** de las fuentes radiactivas. Si ocurriera un intento de acceso o retiro no autorizado, la detección y la evaluación deben darse de manera oportuna para que el personal de respuesta actúe con suficiente tiempo y recursos para lograr interrumpir al adversario y prevenir el retiro de la fuente. Para cumplir con esta meta, se recomiendan las siguientes medidas:

Detección

Objetivo de seguridad: Detección inmediata de todo acceso no autorizado al área o ubicación segura de la fuente

Medidas de seguridad: Sistema electrónico de detección de intrusiones o vigilancia continua por parte del personal del operador.

Los sensores electrónicos que están conectados al sistema de alarmas o vigilancia visual continua por parte del personal del operador indican que hubo un acceso no autorizado al área segura (ver la sección sobre "Demora" más adelante) o a la ubicación de la fuente. Se debería tener el cuidado de garantizar que las medidas de detección de intrusiones no sean ignoradas. Para las fuentes en uso, tales medidas deben detectar el acceso no autorizado al área segura donde se usa la fuente. Para las fuentes en almacenamiento, tales medidas deben detectar el acceso no autorizado a la sala con llave u otra ubicación donde se almacene la fuente. Para fuentes móviles o portátiles en uso, la vigilancia visual continua podría ser el único medio factible para la detección inmediata de intrusiones.

Objetivo de seguridad: Detectar inmediatamente todo intento no autorizado de retiro de la fuente (por ejemplo, por parte de un interno).

Medidas de seguridad: Equipo electrónico de detección de forzamiento o vigilancia continua por parte del personal del operador.

Los sensores electrónicos que están conectados al sistema de alarmas o vigilancia visual continua por parte del personal del operador indican que hubo un intento no autorizado de retiro de la fuente. Se debe tener el cuidado de garantizar que las medidas de detección de forzamiento no sean ignoradas. Para fuentes móviles o portátiles en uso, la vigilancia visual continua podría ser el único medio factible para la detección inmediata de forzamiento. Nótese, sin embargo, que si se elige la vigilancia continua como medida de seguridad, la vigilancia visual continua podría requerir la observación de al menos dos personas en todo momento para protegerse ante un evento ocasionado por un interno.

Objetivo de seguridad: Evaluar inmediatamente la detección.

Medidas de seguridad: Monitoreo remoto del sistema CCTV o evaluación por parte del operador o personal de respuesta.

Una vez que se activa una alarma de detección de intrusiones o forzamiento, se debería evaluar inmediatamente la causa de la alarma. Esta tarea la puede realizar el personal del operador en el lugar donde está la fuente enviando a personas rápidamente a investigar la causa de la alarma o a través del sistema CCTV. Para las fuentes móviles o portátiles en uso, o en casos donde la detección de intrusiones o forzamiento es proporcionada por el personal del operador mediante la vigilancia visual continua, la evaluación se debería realizar de manera simultánea con la detección proporcionada por el personal del operador a cargo de mantener la fuente bajo vigilancia visual continua.

Objetivo de seguridad: Comunicarse inmediatamente con el personal de respuesta.

Medidas de seguridad: Medios de comunicación rápidos, confiables y variados como teléfonos, celulares, localizadores y radios.

Si la evaluación confirma que ha ocurrido un acceso o un intento de retiro no autorizado de la fuente, se debería notificar inmediatamente al personal de respuesta mediante varios (al menos dos) medios de comunicación como teléfonos fijos, automarcadores, celulares, radios o dispositivos de localización.

Objetivo de seguridad: Proporcionar los medios para detectar la pérdida de una fuente mediante la verificación.

Medidas de seguridad: Revisión diaria mediante observaciones físicas, CCTV, dispositivos de detección de forzamiento, etc.

La revisión diaria debe consistir en medidas que verifiquen la presencia de las fuentes y la ausencia de forzamiento. Tales medidas pueden incluir revisiones físicas para asegurarse de que las fuentes estén en su lugar, observación remota a través del sistema CCTV, verificación de sellos y otros dispositivos evidentes de detección de forzamiento evidente y mediciones de radiación u otros fenómenos físicos que garanticen que la fuente esté presente. Para las fuentes en uso, podría bastar con verificar que el dispositivo sea funcional.

Demora

Objetivo de seguridad: Crear suficiente demora después de la detección para que el personal de respuesta interrumpa el retiro no autorizado de la fuente.

Medidas de seguridad: Sistema de al menos dos capas de barreras (por ejemplo, paredes, jaulas) que juntas generen suficiente demora para permitir al personal de respuesta interceptar al adversario.

Un sistema balanceado con al menos dos capas de barreras debería separar a la fuente del personal no autorizado y generar suficiente demora después de la detección para permitir que personal de respuesta intercepte al adversario o le impida retirar la fuente. Para las fuentes que están en uso, tales medidas podrían incluir un dispositivo con cerradura dentro de un área segura para separar a la fuente del personal no autorizado. Para las fuentes que estén en almacenamiento, las medidas podrían incluir un contenedor fijo con cerradura o un dispositivo que guarde la fuente en una sala de almacenamiento con cerradura, esto con el fin de separar a la fuente del personal no autorizado. Para las fuentes móviles que estén en uso, la vigilancia visual continua por parte del personal del operador podría sustituir una o ambas capas de barreras.

Cuadro 6. Medidas recomendadas para el nivel de seguridad A

(meta: prevenir el retiro no autorizado)

Función de seguridad física	Objetivo de seguridad física	Medidas de seguridad
Detección	Detectar inmediatamente todo acceso no autorizado al área segura o la ubicación de la fuente.	Sistema electrónico de detección de intrusiones o vigilancia continua por parte del personal del operador.
	Detectar inmediatamente todo intento de retiro no autorizado de la fuente, incluido el de un interno.	Sistema electrónico de detección de forzamiento o vigilancia continua por parte del personal del operador.
	Evaluar inmediatamente la detección.	Monitoreo remoto del sistema CCTV o evaluación por parte del operador o personal de respuesta.
	Comunicarlo inmediatamente al personal de respuesta.	Medios de comunicación rápidos, confiables y variados como teléfonos, celulares, localizadores y radios.
	Proporcionar los medios para detectar la pérdida de una fuente mediante la verificación.	Revisión diaria mediante revisiones físicas, CCTV, dispositivo de detección de forzamiento, etc.

Función de seguridad física	Objetivo de seguridad física	Medidas de seguridad
Demora	Crear suficiente demora después de la detección para que el personal de respuesta interrumpa el retiro no autorizado.	Sistema de al menos dos capas de barreras (por ejemplo, paredes, jaulas) que brinden suficiente demora para permitirle al personal de respuesta interceptar al adversario.
Respuesta	Responder inmediatamente a una alarma evaluada con suficientes recursos para interrumpir y prevenir el retiro no autorizado.	Capacidad de respuesta inmediata con el número, el equipo y la capacitación necesarias para poder interceptar.
Gestión de la seguridad física	Instalar controles que restrinjan el acceso a ubicación de la fuente únicamente a personas autorizadas.	Identificación y verificación, por ejemplo, mediante cerraduras con lector de tarjetas magnéticas y número de identificación personal o llaves y control de llaves.
	Garantizar la probidad de las personas autorizadas.	Revisión de antecedentes para todo el personal con acceso autorizado sin escolta a la ubicación de la fuente y con acceso a la información sensible.
	Identificar y proteger la información sensible.	Procedimientos para identificar la información sensible y protegerla para que no sea revelada sin autorización

Función de seguridad física	Objetivo de seguridad física	Medidas de seguridad
	Proporcionar un plan de seguridad física.	Un plan de seguridad física que se ajuste a los requisitos reglamentarios y que proporcione la respuesta ante los niveles incrementados de amenaza.
	Garantizar la capacidad para lidiar con eventos de seguridad física incluidos en los planes de contingencia.	Procedimientos para responder a eventos relacionados con la seguridad física.
	Establecer un sistema de reporte de eventos de seguridad física.	Procedimientos para un reporte oportuno de eventos de seguridad física.

Respuesta

Objetivo de seguridad: Responder inmediatamente a una alarma evaluada con suficientes recursos para interrumpir y prevenir el retiro no autorizado.

Medidas de seguridad: Poder proporcionar una respuesta inmediata con el número, el equipo y la preparación de respuesta necesarias para poder interceptar al adversario.

El operador debería crear protocolos para garantizar el despliegue inmediato y sin demora del personal de respuesta para responder a una alarma. Tal respuesta debe ser

inmediata y adecuada. *Inmediata* significa que el personal de respuesta, una vez notificado, debería llegar en menos tiempo que el requerido para sobrepasar las barreras y realizar las acciones necesarias para retirar la fuente. *Adecuada* significa que el equipo de respuesta tiene suficiente número y capacidad para vencer al adversario. La respuesta podría ser un cuerpo de seguridad contratado directamente o subcontratado, la policía local o la gendarmería nacional.

Gestión de la seguridad

Objetivo de seguridad: Instalar controles que les impidan a personas no autorizadas el acceso a la ubicación de la fuente.

Medidas de seguridad: Identificación y verificación de personas, por ejemplo, cerraduras con lector de tarjetas magnéticas y número de identificación personal o llaves y control de llaves.

El control de acceso busca que únicamente las personas autorizadas tengan acceso a la ubicación de la fuente. Con tal medida, las personas autorizadas pueden desactivar temporalmente las barreras físicas, como las puertas con cerraduras (demora), después de verificar la identidad de la persona y la autorización de acceso. (En el contexto de las exposiciones médicas, los pacientes no requieren estar «autorizados» puesto que son escoltados a la fuente y están bajo vigilancia constante por parte del personal médico.)

Las medidas para verificar la identidad y la autorización de una persona que busca obtener el acceso pueden ser las siguientes:

— Número de identificación personal (PIN) para activar el lector de control que está en la puerta.

— Un sistema de credenciales que podría también activar un lector electrónico.

— Un sistema de intercambio de credenciales en un punto de control en la entrada.

— Elementos biométricos para activar un dispositivo de control de puertas.

Una vez verificada la autorización de acceso de la persona, el sistema le permite ingresar al área segura o ubicación de la fuente, por ejemplo, abriendo una cerradura. Se deberían requerir dos o más medidas de verificación, por ejemplo, el uso de una tarjeta magnética y un PIN, una tarjeta magnética y una llave de control, un PIN y una contraseña de computadora o una llave de control y la verificación de identidad por parte de otro miembro del personal autorizado. Para las fuentes en uso, tales medidas deberían controlar el acceso al área donde se usa la fuente. Para las fuentes en almacenamiento, tales medidas deberían controlar el acceso con cerradura a la sala u otra ubicación donde se almacene la fuente. Para las fuentes móviles que estén en uso, la vigilancia visual continua por parte de múltiples miembros del personal del operador podría sustituir el control de acceso.

Objetivo de seguridad: Garantizar la probidad de las personas autorizadas.

Medidas de seguridad: Revisión de antecedentes para todo el personal con acceso autorizado sin escolta a la ubicación de la fuente y con acceso a información sensible.

La probidad de una persona debería evaluarse mediante una revisión satisfactoria de antecedentes antes de permitirle el acceso sin escolta a las fuentes radiactivas, a los lugares donde se utilizan o almacenan o a cualquier información sensible relacionada. La naturaleza y profundidad de tal revisión debería ser proporcional al nivel de seguridad de la fuente radiactiva y de conformidad con las regulaciones del Estado o lo que determine la autoridad reguladora. Como mínimo, se debería confirmar la identidad y verificar las referencias para poder determinar la integridad, el carácter y la probidad de la persona. El proceso debería revisarse regularmente y apoyarse con la constante atención de los supervisores y directores para garantizar que el personal en todos los niveles de la organización actúe de manera responsable y confiable y que la autoridad reguladora esté al tanto de cualquier duda en este contexto.

Objetivo de seguridad: Identificar y proteger la información sensible.

Medidas de seguridad: Procedimientos para identificar la información sensible y protegerla para que no sea revelada sin autorización.

Así como se protegen las fuentes radiactivas, también es necesario proteger la información relacionada con ellas, la cual podría incluir documentos, datos en los sistemas de cómputo y otros medios que puedan usarse para identificar detalles sobre:

— La ubicación específica e inventario de las fuentes.

— El plan de seguridad y los acuerdos de seguridad pertinentes.

— Los sistemas de seguridad (por ejemplo, alarmas contra intrusos), incluidos los diagramas de rendimiento e instalación.

— Las debilidades temporales o a largo plazo del programa de seguridad.

— Los acuerdos del personal de seguridad y los medios para responder a eventos de seguridad o alarmas.

— Las fechas, las rutas y la modalidad planeadas para el transporte o la transferencia de fuentes.

— Los planes de contingencia y medidas de respuesta a eventos de seguridad.

También se deberían aportan directrices reglamentarias para los siguientes aspectos:

— El control, el almacenamiento, la preparación, la identificación, el etiquetado y la transmisión de documentos o correspondencia que contenga información sensible.

— Métodos recomendados para la destrucción de documentos que contengan información sensible.

— Acuerdos que cubran la desclasificación y gestión de documentos una vez que estén obsoletos o dejen de contener información sensible.

Objetivo de seguridad: Proporcionar un plan de seguridad física.

Medidas de seguridad: Un plan de seguridad física que se ajuste a los requisitos reglamentarios y que proporcione respuesta ante los niveles incrementados de amenaza.

Los operadores deberían preparar un plan de seguridad para cada instalación. Para ver ejemplos acerca del contenido de un plan de seguridad, ver el Apéndice II. La autoridad reguladora podría autorizar los planes de seguridad y revisarlos en intervalos establecidos durante el proceso de inspección para garantizar que se adecúen al sistema de seguridad actual. Los planes de seguridad podrían variar para las fuentes de uso móvil o portátil o para fuentes que permanezcan almacenadas entre períodos de uso. Es posible que la mayoría de planes incluyan información sensible sobre los acuerdos de seguridad, por lo que deberían gestionarse como corresponde. El plan de seguridad también debería permitir una transición eficaz y oportuna ante un nivel de seguridad aumentado, esto en caso de que haya un aumento en el grado de amenaza.

Objetivo de seguridad: Garantizar la capacidad para lidiar con eventos de seguridad física incluidos en los planes de contingencia

Medidas de seguridad: Procedimientos para responder a eventos relacionados con la seguridad física.

Cada recinto debería establecer planes de contingencia de seguridad para varios tipos de eventos, entre ellos:

— Una sospecha o amenaza de actos dolosos.

— Una manifestación pública que pueda amenazar las fuentes radiactivas.

— Una intrusión al área segura por parte de personas no autorizadas. Esto puede incluir desde una simple entrada no autorizada hasta un ataque determinado por parte de quienes busquen retirar o interferir con el uso de las fuentes radiactivas.

El operador debería desarrollar escenarios razonablemente predecibles que incluyan tales eventos y procedimientos para responder a ellos. Los planes de contingencia deberían compartirse con las autoridades correspondientes y practicarse en intervalos regulares.

Objetivo de seguridad: Establecer un sistema de reporte de eventos de seguridad.

Medidas de seguridad: Procedimientos para el reporte oportuno de eventos de seguridad.

El operador debería establecer procedimientos para reportar eventos de seguridad a la autoridad reguladora, los primeros actuantes y otros, según sea pertinente, dentro del período que requiera la autoridad reguladora para tomar las acciones que se ajusten a la magnitud del evento en términos de seguridad física. Entre los eventos que se deben reportar, se incluyen los siguientes:

— Las discrepancias en los datos de contabilidad.

— La sospecha de robo o el robo de una fuente radiactiva.

— La intrusión no autorizada a una instalación o área de almacenamiento de una fuente.

— El descubrimiento de un posible explosivo o de un explosivo real cerca de una instalación o centro de almacenamiento.

— La pérdida de control de una fuente radiactiva.

— El acceso o el uso no autorizado de una fuente.

— Otros actos dolosos que amenacen las actividades autorizadas.

— Los eventos o avistamientos sospechosos que puedan indicar que se planea un ataque de sabotaje, una intrusión o el retiro de una fuente.

— La falla o pérdida de sistemas de seguridad física que sean esenciales para la protección de fuentes radiactivas.

Introducción a las medidas de seguridad para el Nivel B

La meta del nivel de seguridad B es **minimizar la posibilidad de un retiro no autorizado** de las fuentes radiactivas. Si ocurriera un intento de acceso o retiro no autorizado, la respuesta debe iniciarse inmediatamente después de la detección y evaluación de la intrusión, pero no se requiere que la respuesta llegue a tiempo para prevenir el retiro de la fuente. Para cumplir con esta meta, se recomiendan las siguientes medidas:

Detección

Objetivo de seguridad: Detectar inmediatamente todo acceso no autorizado al área o ubicación segura de la fuente.

Medidas de seguridad: Equipo electrónico de detección de intrusiones o vigilancia continua por parte del personal del operador.

Los sensores electrónicos que están conectados a una alarma o sistema de vigilancia visual continua por parte del personal del operador indican el acceso no autorizado al área segura (ver la sección sobre "Demora" más adelante) o a la ubicación de la fuente. Se debería tener el cuidado de garantizar que las medidas de detección de intrusiones no sean excluidas. Para las fuentes en uso, tales medidas deben detectar el acceso no autorizado al área segura donde se usa la fuente. Para las fuentes en almacenamiento, tales medidas deben detectar el acceso no autorizado a la sala con cerradura o a la ubicación donde esté almacenada la fuente. Para fuentes móviles o portátiles en uso, la vigilancia visual continua podría ser el único medio factible para la detección de intrusiones.

Objetivo de seguridad: Detectar todo intento de retiro no autorizado de la fuente

Medidas de seguridad: Equipo de detección de forzamiento o revisiones periódicas por parte del personal del operador.

El equipo de detección de forzamiento o vigilancia visual continua por parte del personal del operador realizada durante las revisiones periódicas indica el intento de retiro no autorizado

de la fuente. Se debería tener el cuidado de garantizar que las medidas de detección de forzamiento no sean excluidas. Esto puede facilitarse mediante el uso del equipo electrónico de detección de forzamiento. Para fuentes móviles o portátiles en uso, la vigilancia visual continua podría ser el único medio factible para la detección de forzamiento.

Objetivo de seguridad: Evaluar inmediatamente la detección.

Medidas de seguridad: Monitoreo remoto del sistema CCTV o evaluación por parte del personal del operador o de respuesta.

Una vez que se activa una alarma de detección de intrusiones, se debería evaluar inmediatamente su causa. Esta tarea la puede realizar el personal del operador en la ubicación de la fuente mediante el envío inmediato de personas para que investiguen la causa de la alarma o mediante el sistema CCTV. Para las fuentes móviles o portátiles en uso, o en casos en los que la detección de intrusiones o forzamiento es proporcionada por el personal del operador mediante la vigilancia visual continua, la evaluación se debe realizar de manera simultánea con la detección indicada por el personal del operador a cargo de mantener la fuente bajo vigilancia visual continua.

Objetivo de seguridad: Comunicarse de inmediato con el personal de respuesta.

Medidas de seguridad: Medios de comunicación rápidos y confiables como teléfonos, celulares, localizadores y radios.

Si la evaluación confirma que ha ocurrido un acceso o retiro no autorizado de la fuente, se debe notificar inmediatamente al personal de respuesta mediante medios de comunicación confiables como teléfonos fijos, automarcadores, celulares, radios o dispositivos de localización.

Cuadro 7. Medidas recomendadas para el nivel de seguridad B

(meta: minimizar la posibilidad de un retiro no autorizado de una fuente)

Función de seguridad física	Objetivo de seguridad física	Medidas de seguridad
Detección	Evaluar inmediatamente la detección	Monitoreo remoto del sistema CCTV o evaluación por parte del personal del operador o de respuesta.
	Comunicar inmediatamente al personal de respuesta	Medios de comunicación rápidos y confiables como teléfonos, celulares, localizadores y radios.
	Proporcionar los medios para detectar la pérdida de una fuente mediante verificación.	Revisiones semanales mediante revisiones físicas, equipo de detección de forzamiento, etc.
Demora	Crear demora para minimizar la posibilidad de un retiro no autorizado	Sistema de dos capas de barreras (por ejemplo, paredes, jaulas)
Respuesta	Iniciar inmediatamente la respuesta para interrumpir el retiro no autorizado	Equipo y procedimientos para iniciar inmediatamente la respuesta
Gestión de la Seguridad	Instalar controles que limiten eficazmente el acceso a la ubicación de la fuente únicamente a personas autorizadas	Medida de una sola identificación
	Garantizar la probidad de las personas autorizadas	Revisión de antecedentes para todo el personal con acceso autorizado sin escolta a la ubicación de la fuente y con acceso a la información sensible.
	Identificar y proteger la información sensible	Procedimientos para identificar la información sensible y protegerla para que no sea revelada sin autorización
	Proporcionar un plan de seguridad física	Un plan de seguridad física que se ajuste a los requisitos reglamentarios y proporcione la respuesta ante niveles aumentados de amenaza
	Garantizar la capacidad para lidiar con eventos de seguridad física incluidos en los planes de contingencia	Procedimientos para responder a eventos relacionados con la seguridad física.
	Establecer un sistema de reporte de eventos de seguridad	Procedimientos para un reporte oportuno de eventos de seguridad.

Objetivo de seguridad: Proporcionar los medios para detectar la pérdida de una fuente mediante la verificación.

Medidas de seguridad: Revisiones semanales mediante observaciones físicas, equipo de detección de forzamiento, etc.

La revisión semanal consiste en medidas para garantizar que las fuentes estén presentes y que no hayan sido forzadas. Tales medidas pueden incluir revisiones físicas, verificación de sellos y otros dispositivos evidentes de forzamiento y mediciones de radiación u otros fenómenos físicos que garanticen que la fuente está presente. Para las fuentes en uso, verificar que el dispositivo esté en funcionamiento puede ser suficiente.

Demora

Objetivo de seguridad: Crear demora para minimizar la posibilidad de un retiro no autorizado

Medidas de seguridad: Sistema de dos capas de barreras (por ejemplo, paredes, jaulas)

Un sistema balanceado de dos barreras debería separar la fuente del personal no autorizado. Para las fuentes que estén en uso, tales medidas podrían incluir un dispositivo con cerradura en un área segura que separe la fuente del personal no autorizado. Para las fuentes que estén en almacenamiento, las medidas podrían incluir un contenedor fijo con cerradura o un dispositivo que guarde la fuente y una sala de almacenamiento con cerradura que separe la fuente del personal no autorizado. Para las fuentes móviles que estén en uso, la vigilancia visual continua por parte del personal del operador podría sustituir las barreras.

Respuesta

Objetivo de seguridad: Iniciar inmediatamente la respuesta para interrumpir el retiro no autorizado.

Medidas de seguridad: Equipo y procedimientos para iniciar de inmediato la respuesta.

El operador debería establecer protocolos para garantizar el despliegue inmediato y sin demora de personal para responder a una alarma y bloquear al adversario. La respuesta puede ser un cuerpo de seguridad contratado directamente o subcontratado, la policía local o la gendarmería nacional. La respuesta debería coordinarse con las autoridades locales para mitigar las posibles consecuencias.

Gestión de la seguridad

Objetivo de seguridad: Establecer controles que restrinjan eficazmente el acceso a la ubicación de la fuente únicamente a personas autorizadas.

Medidas de seguridad: Medidas de una sola identificación.

El propósito del control de acceso es restringir el acceso a la ubicación de la fuente únicamente a personas autorizadas. Por lo general, tal medida se cumple cuando se permite a tales personas desactivar temporalmente las barreras físicas, como las puertas con cerraduras (medidas de demora), después de haber verificado su identidad y la autorización de acceso (en el caso de las exposiciones médicas, los pacientes no requieren estar "autorizados").

Algunas medidas para verificar la identidad y la autorización de una persona que busca obtener acceso son las siguientes:

— Un PIN para activar el lector de control de la puerta.

— Un sistema de credenciales que podría activar también un lector electrónico.

— Un sistema de intercambio de credenciales en un punto de control de entrada.

— Elementos biométricos para activar un dispositivo de control de puertas.

Una vez verificada la autorización de acceso de la persona, el sistema le permitiría ingresar al área segura o a la ubicación de la fuente, por ejemplo, abriéndole una cerradura. Se debería requerir al menos una medida de identificación, por ejemplo, el uso de una tarjeta magnética, un PIN, una contraseña de computadora, una llave de control o la verificación visual

de la identidad de la persona por parte de otro miembro del personal autorizado. Para las fuentes en uso, tales medidas deberían controlar el acceso al área donde se usa la fuente. Para las fuentes en almacenamiento, tales medidas deberían controlar el acceso a la sala con cerradura u otra ubicación donde se almacene la fuente. Para las fuentes móviles o portátiles que estén en uso, la vigilancia visual continua por parte del personal del operador podría sustituir el control de acceso.

Objetivo de seguridad: Garantizar la probidad de las personas autorizadas.

Medidas de seguridad: Revisión de antecedentes para todo el personal con acceso autorizado sin escolta a la ubicación de la fuente y con acceso a la información sensible.

La probidad de una persona debería ser evaluada mediante un estudio satisfactorio de antecedentes antes de permitirle el acceso sin escolta a las fuentes radiactivas, los lugares donde se utilizan o almacenan las fuentes o a cualquier información sensible relacionada. La naturaleza y profundidad de tal estudio deberían ser proporcionales al nivel de seguridad de la fuente radiactiva y de conformidad con las regulaciones del Estado o lo que determine la autoridad reguladora. Como mínimo, se debería incluir la confirmación de la identidad y la verificación de las referencias para determinar la integridad, personalidad y probidad de cada persona. El proceso debería ser revisado y apoyado por la constante atención por parte de los supervisores y directores para garantizar que el personal de todos los niveles actúe de manera responsable y confiable y que la autoridad pertinente esté al tanto de cualquier asunto importante dentro de este contexto.

Objetivo de seguridad: Identificar y proteger la información sensible.

Medidas de seguridad: Procedimientos para identificar la información sensible y protegerla para que no sea revelada sin autorización.

Además de proteger las fuentes radiactivas, el sistema de seguridad física también debería proteger la información relacionada con ellas, la cual podría incluir documentos, datos en los sistemas de las computadoras y otros medios que se puedan usar para identificar detalles relacionados con:

— La ubicación y el inventario específicos de las fuentes.

— El plan de seguridad pertinente y los acuerdos sobre seguridad.

— Los sistemas de seguridad (por ejemplo, alarmas de intrusiones), incluidos los diagramas de rendimiento e instalación.

— Las debilidades temporales o a largo plazo del programa de seguridad.

— Los acuerdos del personal de seguridad y los medios para responder a eventos de seguridad o alarmas.

— Las fechas, las rutas y la modalidad para el transporte o transferencia de fuentes que se planean utilizar.

— Planes de contingencia y medidas de respuesta ante eventos de seguridad física.

Las directrices reglamentarias también deberían incluir información sobre:

— El control, el almacenamiento, la preparación, la identificación, el etiquetado y la transmisión de documentos o correspondencia que contenga información sensible.

— Los métodos recomendados para la destrucción de documentos que contengan información sensible.

— Las disposiciones en cuanto a la desclasificación y gestión de documentos una vez que sean obsoletos o dejen de contener información sensible.

Objetivo de seguridad: Proporcionar un plan de seguridad física.

Medidas de seguridad: Un plan de seguridad física que se ajuste a los requisitos reglamentarios y que posibilite la respuesta ante niveles aumentados de amenaza.

Cada operador debería elaborar un plan de seguridad en cada instalación. Para ver ejemplos sobre un plan de seguridad, ver el Apéndice II. La autoridad reguladora podría autorizar los planes de seguridad y revisarlos en intervalos establecidos durante el proceso de inspección con el fin de garantizar que se ajusten al sistema de seguridad física actual. Los planes podrían variar para las fuentes de uso móvil o portátil o para fuentes que permanezcan almacenadas entre períodos de uso. Es posible que la mayoría de planes incluyan información sensible sobre los acuerdos de seguridad, por lo que deberían ser gestionados como corresponde. El plan de seguridad también debería permitir una transición oportuna a un nivel de seguridad aumentado, esto en caso de que haya un aumento en el nivel de amenaza.

Objetivo de seguridad: Garantizar la capacidad para lidiar con eventos de seguridad física incluidos en los planes de contingencia.

Medidas de seguridad: Procedimientos para responder a eventos relacionados con la seguridad física.

Cada instalación debería establecer planes de contingencia de seguridad para varios tipos de eventos, entre ellos:

— Una sospecha o amenaza de actos dolosos.

— Una manifestación pública que tenga el potencial de amenazar las fuentes radiactivas.

— Una intrusión por parte de personas no autorizadas al área segura. Esto puede abarcar desde una simple entrada no autorizada hasta un ataque premeditado por parte de quienes busquen retirar o interferir con el uso de las fuentes radiactivas.

El operador debería desarrollar escenarios razonablemente predecibles que incluyan tales eventos y los procedimientos para responder a ellos. Los planes de contingencia deberían compartirse con las autoridades correspondientes y ponerse en práctica en intervalos regulares.

Objetivo de seguridad: Establecer un sistema de reporte de eventos de seguridad.

Medidas de seguridad: Procedimientos para un reporte oportuno de eventos de seguridad.

El operador debería establecer procedimientos para reportar eventos de seguridad física a la autoridad reguladora, los primeros actuantes y otros, según sea pertinente, dentro del período que requiera la autoridad reguladora para tomar las acciones que se ajusten a la magnitud del evento en términos de seguridad física. Entre los eventos que se deben reportar, se incluyen:

— Discrepancias en los datos de contabilidad.

— Sospecha de robo o robo de una fuente radiactiva.

— Intrusión no autorizada a una instalación o área de almacenamiento de la fuente.

— Descubrimiento de un posible explosivo o un explosivo cerca de una instalación o centro de almacenamiento.

— Pérdida de control de una fuente radiactiva.

— Acceso o uso no autorizado de una fuente.

— Otros actos dolosos que atenten contra las actividades autorizadas.

— Eventos o avistamientos sospechosos que puedan indicar que se planea un ataque de sabotaje, una intrusión o el retiro de una fuente.

— Falla o pérdida de sistemas de seguridad que sean esenciales para la protección de fuentes radiactivas.

Introducción a las medidas de seguridad para el nivel C

La meta del nivel de seguridad C es **reducir la posibilidad de un retiro no autorizado** de las fuentes radiactivas. Para cumplir con esta meta, se recomiendan las siguientes medidas.

Detección

Objetivo de seguridad: Detectar el retiro no autorizado de la fuente.

Medidas de seguridad: Equipo de detección de forzamiento o revisiones periódicas por parte del personal del operador.

Los operadores deben verificar que las fuentes estén presentes. Las medidas podrían incluir revisiones físicas para asegurarse de que las fuentes estén en su lugar, verificación de sellos y otros dispositivos de detección de forzamiento y mediciones de radiación u otros elementos físicos que garanticen que la fuente esté presente. En el caso de las fuentes en uso, podría bastar con verificar que el dispositivo esté en funcionamiento.

Objetivo de seguridad: Evaluar de inmediato la detección.

Medidas de seguridad: Evaluación por parte del personal del operador o de respuesta.

Una vez que se indique que la fuente no está presente mediante la detección de forzamiento o la revisión visual, se debe evaluar la situación de inmediato para determinar si en realidad ha ocurrido un retiro no autorizado.

Objetivo de seguridad: Proporcionar los medios para detectar la pérdida de una fuente mediante la verificación.

Medidas de seguridad: Revisión mensual mediante revisiones físicas, dispositivos de detección de forzamiento, etc.

La revisión mensual consiste en medidas que aseguren que las fuentes están presentes y que no han sido forzadas. Las medidas podrían incluir revisiones físicas para asegurarse de que las fuentes estén en su lugar, verificación de sellos y otros dispositivos de detección de forzamiento y mediciones de radiación u otros fenómenos físicos que garanticen que la fuente está presente. Para las fuentes en uso, el verificar que el dispositivo sea funcional puede ser suficiente.

Demora

Objetivo de seguridad: Crear demora para reducir la posibilidad de un retiro no autorizado de la fuente.

Medidas de seguridad: Una barrera (por ejemplo, una jaula o caja protectora para la fuente) u observación del personal del operador.

Como mínimo, una barrera debería separar a la fuente del personal no autorizado. Para las fuentes en uso, tales medidas podrían incluir la caja protectora de la fuente o utilizar la fuente en un área segura. Para las fuentes que están en almacenamiento, las medidas podrían incluir un contenedor fijo con cerradura, un dispositivo que guarde la fuente o una sala de almacenamiento con cerradura que separe a la fuente del personal no autorizado. Para las fuentes móviles que estén en uso, la vigilancia visual continua por parte del personal del operador podría sustituir la barrera.

Respuesta

Objetivo de seguridad: Poner en práctica las acciones adecuadas en caso de un retiro no autorizado de una fuente.

Medidas de seguridad: Procedimientos para identificar las acciones necesarias con base en los planes de contingencia.

Los procedimientos normativos deberían garantizar que se evalúe cualquier sospecha de retiro no autorizado o pérdida de una fuente y que, de confirmarse, sea reportada de inmediato a la autoridad pertinente. Esto debería ir seguido de un esfuerzo por localizar y recuperar la fuente e investigar las circunstancias que llevaron a tal evento.

Gestión de la seguridad

Objetivo de seguridad: Instalar controles que restrinjan el acceso a la ubicación de la fuente únicamente a personas autorizadas.

Medidas de seguridad: Medidas de una sola identificación.

CUADRO 8. Medidas recomendadas para el nivel de seguridad C

(meta: reducir la posibilidad de un retiro no autorizado de una fuente)

Función de seguridad	Objetivo de seguridad física	Medidas de seguridad
Detección	Detectar el retiro no autorizado de la fuente.	Equipo de detección de forzamiento o revisiones periódicas por parte del personal del operador.
	Evaluar de inmediato la detección.	Evaluación por parte del personal del operador o de respuesta.
	Proporcionar los medios para detectar la pérdida de una fuente mediante la verificación.	Revisiones mensuales mediante revisiones físicas, dispositivos de detección de forzamiento u otros medios para confirmar la presencia de la fuente.
Demora	Crear demora para reducir la posibilidad de un retiro no autorizado de la fuente.	Una barrera (por ejemplo, una jaula o caja protectora para la fuente) o bajo observación del personal del operador.
Respuesta	Poner en práctica las acciones adecuadas en caso de un retiro no autorizado de una fuente.	Procedimientos para identificar las acciones necesarias con base en los planes de contingencia.
	Instalar controles que limiten el acceso a la ubicación de la fuente únicamente a personas	Medidas de una sola identificación.

Función de seguridad	Objetivo de seguridad física	Medidas de seguridad
	autorizadas.	
Gestión de la seguridad	Garantizar la probidad de las personas autorizadas.	Métodos adecuados para determinar la probidad de las personas con acceso autorizado sin escolta a la ubicación de la fuente y con acceso a la información sensible.
	Identificar y proteger la información sensible.	Procedimientos para identificar la información sensible y protegerla para que no sea revelada sin autorización.
	Proporcionar un plan de seguridad física.	Documentación de los acuerdos de seguridad y procedimientos de referencia.
	Garantizar la capacidad para lidiar con eventos de seguridad física incluidos en los planes de contingencia.	Procedimientos para responder a eventos relacionados con la seguridad física.
	Establecer un sistema de reporte de eventos de seguridad.	Procedimientos para un reporte oportuno de eventos de seguridad física.

El control de acceso busca que únicamente las personas autorizadas tengan acceso a la ubicación de la fuente. Por lo general, tal medida se cumple cuando se permite a tales personas desactivar temporalmente las barreras físicas, como las puertas con cerraduras (medidas de demora), después de verificar la identidad de la persona y la autorización de acceso (en el caso de las exposiciones médicas, los pacientes no requieren estar "autorizados").

Las medidas para verificar la identidad y la autorización de una persona que busca obtener acceso son las siguientes:

— Un PIN para activar el lector de control de la puerta.

— Un sistema de credenciales que también podría activar un lector electrónico.

— Un sistema de intercambio de credenciales en un punto de control de entrada.

— Elementos biométricos para activar un dispositivo de control de puertas.

Una vez verificada la autorización del acceso de la persona, el sistema le permitiría ingresar al área segura o ubicación de la fuente, por ejemplo, abriendo una cerradura. Se debería requerir al menos una medida de identificación, por ejemplo, el uso de una tarjeta magnética, un PIN, una contraseña de computadora, una llave de control o la verificación visual de la identidad de la persona por parte de otro miembro del personal autorizado. Para las fuentes en uso, tales medidas deberían controlar el acceso al área donde se utiliza la fuente. Para las fuentes en almacenamiento, tales medidas deberían controlar el acceso a la sala con cerradura u otra ubicación donde se almacene la fuente. Para las fuentes móviles que estén en uso, la vigilancia visual continua por parte del personal del operador podría sustituir el control de acceso.

Objetivo de seguridad: Garantizar la probidad de las personas autorizadas.

Medidas de seguridad: Métodos adecuados para determinar la probidad de las personas con acceso autorizado sin escolta a la ubicación de la fuente y con acceso a información sensible.

La probidad de una persona se debería evaluar mediante una revisión satisfactoria de antecedentes antes de permitirle el acceso sin escolta a las fuentes radiactivas, a los lugares donde se utilizan o almacenan o a cualquier información sensible relacionada. La naturaleza y profundidad de tal revisión debería ser proporcional al nivel de seguridad de la fuente radiactiva y de conformidad con los estándares del Estado o lo que determine la autoridad reguladora.

Objetivo de seguridad: Identificar y proteger la información sensible.

Medidas de seguridad: Procedimientos para identificar la información sensible y protegerla para que no sea revelada sin autorización.

Las disposiciones normativas deben garantizar que el operador evalúe si las personas con acceso a la información relacionada con la seguridad o a las fuentes radiactivas son confiables. Si no se ha determinado su probidad, no se les debería conceder el acceso sin escolta.

Objetivo de seguridad: Proporcionar un plan de seguridad física.

Medidas de seguridad: Documentación de los acuerdos de seguridad física y procedimientos de referencia.

Las disposiciones de seguridad física y los procedimientos de referencia deberían adoptarse en la forma de un plan de seguridad física. Para ver ejemplos de uno de estos planes, ver el Apéndice II.

Objetivo de seguridad: Garantizar la capacidad para lidiar con eventos de seguridad física incluidos en los planes de contingencia.

Medidas de seguridad: Procedimientos para responder a eventos relacionados con la seguridad física.

La declaración de seguridad debería indicar los procedimientos para investigar y reportar cualquier acceso o retiro no autorizado de una fuente.

Objetivo de seguridad: Establecer un sistema de notificación de eventos de seguridad física.

Medidas de seguridad: Procedimientos para la notificación oportuna de eventos de seguridad física.

El operador debería establecer procedimientos para notificar eventos de seguridad física a la autoridad reguladora, los primeros actuantes y otros, según sea pertinente, dentro del período que requiera la autoridad reguladora para tomar acciones de acuerdo con la importancia del evento en términos de seguridad física. Entre los eventos que se deben notificar, se incluyen los siguientes:

— Las discrepancias en los datos de contabilidad.

— La sospecha de robo o robo de una fuente radiactiva.

— La intrusión no autorizada a una instalación o área de almacenamiento de la fuente.

— El descubrimiento de un posible explosivo o un explosivo cerca de una instalación o centro de almacenamiento.

— La pérdida de control de una fuente radiactiva.

— El acceso o uso no autorizado de una fuente.

— Otros actos dolosos que atenten contra las actividades autorizadas.

— Los eventos o avistamientos sospechosos que puedan indicar que se planea un ataque de sabotaje, una intrusión o un retiro de una fuente.

— La falla o pérdida de sistemas de seguridad que sean esenciales para la protección de fuentes radiactivas.

4.3.2. Enfoque basado en el desempeño

La autoridad reguladora podría decidir utilizar un enfoque basado en el desempeño mediante el cual los operadores cumplan con los objetivos de seguridad pertinentes. Normalmente, el enfoque que elija un Estado dependerá del grado de experticia de la autoridad reguladora y el operador en materia de seguridad física. Un enfoque basado en el desempeño funcionaría de forma más eficaz si los operadores cuentan con asesores profesionales y la experticia para diseñar e implementar las medidas necesarias y cuando hayan demostrado registros continuos de consistencia y cumplimiento de la normativa. La autoridad reguladora debería garantizar que las medidas aprobadas estén se hayan documentado de manera clara, por ejemplo en un plan de seguridad física, y hayan sido evaluadas en intervalos adecuados.

Para el enfoque basado en el desempeño, los Estados requerirán el uso de la evaluación de la amenaza nacional y también podrían crear una amenaza base de diseño cuando sea pertinente. La autoridad reguladora debería además especificar un objetivo de seguridad para las clases de fuente a las que aplica el enfoque. En general, tales objetivos de seguridad deberían quedar establecidos en términos de la eficacia requerida del sistema, tal como se describe en la Sección 3.

Se debería crear un sistema de seguridad física que cumpla con los objetivos pertinentes mediante una prueba de vulnerabilidad con respecto a la amenaza base de diseño o la amenaza evaluada. Dependiendo de las circunstancias, la autoridad reguladora o el operador llevarían a cabo esta evaluación mediante el uso del enfoque descrito en la Sección 3 u otra metodología, según lo determine la autoridad reguladora. También se podrían utilizar los resultados de la prueba de vulnerabilidad u otra metodología para demostrar que, de hecho, el sistema de seguridad física resultante cumple con los objetivos de seguridad pertinentes.

La serie de medidas de seguridad física desarrolladas para una fuente en particular según el enfoque basado en el desempeño no necesariamente corresponderían con las

medidas recomendadas en los cuadros 6, 7 y 8 del enfoque prescriptivo. Si bien se incluirían las medidas de seguridad que abordan las funciones de seguridad de *detección*, *demora* y *respuesta* del Cuadro 2, la combinación particular de medidas variaría según el análisis específico de la situación realizado en la prueba de vulnerabilidad. La aplicación de un enfoque basado en el desempeño en general da como resultado una serie de medidas de seguridad física mejor adaptadas y más económicas que las que se puedan derivar del enfoque prescriptivo. El enfoque basado en el desempeño no se presta para un análisis estadístico de la *disuasión* o *gestión de la seguridad*, aunque estas funciones sean una parte integral del programa. En consecuencia, el enfoque basado en el desempeño también debería tener como requisito la aplicación de medidas de disuasión y gestión de la seguridad física adecuadas al nivel de seguridad física de las fuentes a las que cubre, según se indica en el material relacionado con el enfoque basado en el desempeño. El enfoque basado en el desempeño debería considerar la interacción sistemática entre la detección, la demora y la respuesta para determinar la eficacia general del sistema frente a la amenaza evaluada.

La eficacia del sistema es la medida clave del enfoque basado en el desempeño. Para diseñar un sistema de seguridad usando el enfoque basado en el desempeño, se debe suponer que toda medida de disuasión fallará y que se intenta llevar a cabo un acto doloso. Por lo tanto, el sistema de seguridad deberá diseñarse para que alcance el nivel de eficacia requerido para prevenir el acto doloso que se supone ocurrirá con base en la amenaza evaluada.

4.3.3. Enfoque combinado

Algunos Estados podrían preferir combinar aspectos del enfoque prescriptivo y del basado en el desempeño para poder aplicar medidas de seguridad que cumplan con los objetivos de seguridad indicados anteriormente. Por ejemplo, un Estado podría utilizar el enfoque prescriptivo para las fuentes radiactivas que causarían consecuencias menos graves

si se utilizaran en actos dolosos, pero aplicar el enfoque basado en el desempeño para las fuentes más peligrosas. Para esas fuentes, el Estado realizaría una evaluación de la amenaza nacional y crearía una amenaza base de diseño. Como resultado, el operador sería responsable de aplicar las medidas de seguridad adecuadas para cumplir con una serie de objetivos de seguridad física definidos con base en las funciones de seguridad de *disuasión*, *detección*, *demora*, *respuesta* y *gestión de la seguridad*.

Referencias

[1] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Código de Conducta sobre seguridad tecnológica y física de las fuentes radiactivas, IAEA/CODEOC/2004, OIEA, Viena (2004).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources (Interim Guidance for Comment), IAEA-TECDOC-1355, IAEA, Vienna (2003).

[3] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Clasificación de las fuentes radiactivas, Colección de Normas de Seguridad del OIEA No RS-G-1.9, OIEA, Viena (2009).

[4] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Seguridad de los generadores de radiación y de las fuentes radiactivas selladas, Colección de Normas de Seguridad del OIEA No. RS-G-1.10, OIEA, Viena (2009).

[5] ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA ALIMENTACIÓN Y LA AGRICULTURA, ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, ORGANIZACIÓN INTERNACIONAL DEL TRABAJO, AGENCIA PARA LA ENERGÍA NUCLEAR DE LA OCDE, ORGANIZACIÓN PANAMERICANA DE LA SALUD, ORGANIZACIÓN MUNDIAL DE LA SALUD, Normas básicas internacionales de seguridad para la protección contra la radiación ionizante y para la seguridad de las fuentes de radiación, Colección Seguridad No 115, OIEA, Viena (1997).

[6] COMUNIDAD EUROPEA DE LA ENERGÍA ATÓMICA, ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA ALIMENTACIÓN Y LA AGRICULTURA, ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, ORGANIZACIÓN INTERNACIONAL DEL TRABAJO, ORGANIZACIÓN MARÍTIMA INTERNACIONAL, AGENCIA PARA LA ENERGÍA NUCLEAR DE LA OCDE, ORGANIZACIÓN PANAMERICANA DE LA SALUD, PROGRAMA DE LAS NACIONES UNIDAS PARA EL MEDIO AMBIENTE,

ORGANIZACIÓN MUNDIAL DE LA SALUD, Principios fundamentales de seguridad, Colección de Normas de Seguridad del OIEA No SF-1, OIEA, Viena (2007).

[7] Convenio internacional para la represión de los actos de terrorismo nuclear, Naciones Unidas, Nueva York (2005).

[8] Convención sobre la protección física de los materiales nucleares, INFCIRC/274/Rev.1, OIEA, Viena (1980); Enmienda CPPNM, GOV/INF/2005/10–GC(49)/INF/6, OIEA, Viena (2005).

[9] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Preparación y respuesta a situaciones de emergencia nuclear o radiológica, Colección de normas de seguridad del OIEA No. GS-R-2, OIEA, Viena (2002).

[10] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Proceso de rehabilitación de zonas afectadas por actividades y accidentes pasados, Colección de normas de seguridad del OIEA No. WS-R-3, OIEA, Viena (2009).

[11] INTERNATIONAL COMMISION ON RADIOLOGICAL PROTECTION, Protecting People against Radiation Exposure in the Event of A Radiological Attack Publication 96, Pergamon Press, Oxford (2005).

[12] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, La seguridad en el transporte de materiales radiactivos, Colección de Seguridad Física Nuclear del OIEA No. 9, OIEA, Viena (2008).

[13] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Viena (2009).

[14] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[15] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[16] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Infraestructura legal y estatal para la seguridad nuclear, radiológica, de los desechos radiactivos y del transporte, Colección de normas de seguridad del OIEA No. GS-R-1, OIEA, Viena (2004).

[17] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Cantidades peligrosas de materiales radiactivos (valores D), OIEA, Viena (2010).

[18] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Glosario de Seguridad Tecnológica del OIEA: Terminología empleada en seguridad tecnológica nuclear y protección radiológica, OIEA, Viena (2007), http://www-ns.iaea.org/standards/safety-glossary.asp.

[19] Protección física de los materiales y las instalaciones nucleares, INFCIRC/225/Rev.4 (Corregido), OIEA, Viena (1999).

Definiciones

Acto doloso. Actividad o acto ilícito que se lleva a cabo o en el que se participa de manera intencional y sin justificación ni excusa legal (por ejemplo, contrabando) o un acto o actividad que tenga la intención de causar la muerte, daños físicos o daños materiales a una persona (por ejemplo, un robo) o daños a la propiedad o el ambiente (tomado de GOV/2002/10).

Almacenamiento. La contención de fuentes radiactivas en una instalación con el fin de recuperarlas (tomado de la Ref. [1]).[NT]

Amenaza base de diseño. Descripción detallada de las motivaciones, intenciones y capacidades de los potenciales adversarios frente las cuales se diseñaron y evaluaron los sistemas de seguridad (tomado de la Ref. [13]).

Autoridad reguladora: Entidad, organización o conjunto de entidades u organizaciones a las que el gobierno de un Estado confiere facultades legales para ejercer el control reglamentario en lo concerniente a las fuentes radiactivas, incluida la concesión de autorizaciones y, de este modo, reglamentar uno o más aspectos de la seguridad radiológica y física de las fuentes radiactivas (tomado de la Ref. [1]). [NT]

Autorización. Documento a través del cual la autoridad reguladora otorga un permiso a una persona que ha presentado una solicitud para gestionar una fuente radiactiva. La autorización puede adoptar la forma de un registro, una licencia u otras medidas eficaces de control legal que cumplan con los objetivos del *Código de Conducta* (tomado de la Ref. [1]).[NT]

Cultura de la seguridad física. Características y actitudes de las organizaciones y personas que determinan que las cuestiones de seguridad física reciban la atención que merecen según su importancia (tomado de la Ref. [1]).[NT]

Evaluación de la amenaza. Análisis que documenta las motivaciones, intenciones y capacidades que se crea puedan tener los posibles adversarios y que podrían causar

[NT] Definiciones adaptadas del *Glosario de seguridad tecnológica del OIEA*.

consecuencias indeseables en lo concerniente al material radiactivo en uso o almacenamiento y sus instalaciones conexas (tomado de la Ref. [12]).

Fuente en desuso. Fuente radiactiva que ya no se utiliza y no se tiene la intención de utilizar en las instalaciones y las actividades para las cuales se otorgó la autorización (tomado de la Ref. [18]).[NT1]

Fuente radiactiva. Material radiactivo que se encuentra permanentemente encapsulado o fuertemente consolidado y que no está exento del control regulatorio. También comprende todo material radiactivo que haya sido liberado por fuga o rotura de la fuente radiactiva, pero no así el material encapsulado para su disposición final ni el material nuclear que interviene en los ciclos del combustible nuclear de los reactores de investigación y de potencia (tomado de la Ref. [1]).[NT2]

Operador. Cualquier organización o persona que solicita una certificación, tiene la certificación o es responsable de la seguridad nuclear, radiológica, de los desechos radiactivos o del transporte cuando lleve a cabo sus actividades o tenga relación con instalaciones nucleares o fuentes de radiación ionizante. Puede incluir particulares, organismos gubernamentales, remitentes o transportistas, titulares de licencia, hospitales, trabajadores por cuenta propia, etc. (tomado de la Ref. [18]).[NT1]

Plan de contingencia de seguridad física. Parte del plan de seguridad física o un documento aparte que determina los eventos de seguridad razonablemente previsibles, indica las primeras acciones a tomar (incluido alertar a las autoridades pertinentes) y asignar responsabilidades al personal del operador y de respuesta pertinentes.

Plan de seguridad física. Documento, preparado por el operador y que posiblemente requiera ser revisado por la autoridad reguladora, que presenta una descripción detallada de los acuerdos de seguridad vigentes en una instalación.

[NT1] Definiciones adaptadas del *Glosario de seguridad tecnológica del OIEA*.
[NT2] Definiciones adaptadas del *Código de Conducta*.

Prueba de vulnerabilidad. Proceso que evalúa y documenta las características y la eficacia del sistema de seguridad física global en una instalación en particular.

Retiro no autorizado. Robo u otra sustracción ilícita de fuentes radiactivas (adaptado de la Ref. [19]).

Sabotaje. Daño intencional. En este contexto, sabotaje significa daño intencional a una fuente radiactiva en uso, en almacenamiento o en transporte o a una instalación conexa. También se define como un acto deliberado cometido en perjuicio de una fuente radiactiva en uso, en almacenamiento o en transporte, que pueda poner en peligro, directa o indirectamente, la salud y la seguridad del personal, el público o el medio ambiente mediante la exposición a la radiación o emisión de sustancias radiactivas (tomado de la Ref. [19]).

Seguridad física (nuclear). Prevención y detección de robo, sabotaje, acceso no autorizado, transferencia ilegal u otros actos dolosos relacionados con material nuclear, otras sustancias radiactivas o sus instalaciones conexas y la respuesta a tales actos (tomado de la Ref. [12]). [NT]

[NT] Definiciones adaptadas del *Glosario de seguridad tecnológica del OIEA*.

El informe de investigación

Introducción

Título y presentación general del proyecto de investigación

El título del proyecto es el siguiente: Estrategias adecuadas de documentación para la traducción de guías de seguridad física de fuentes radiactivas.

El presente trabajo consiste en la traducción al español de una guía de implementación para la seguridad física de fuentes radiactivas y el análisis de los métodos de documentación aplicables para su realización. En concreto, se tradujeron seis secciones de la *IAEA Nuclear Security Series No. 11: Implementing Guide. Security of Radioactive Sources* (en adelante guía *Security of Radioactive Sources*). Este texto fue publicado por el International Atomic Energy Agency (IAEA, por sus siglas en inglés)[1] en el 2009 con el propósito de servir de base en la preparación de reglamentos nacionales e institucionales relacionados con la seguridad de las fuentes radiactivas.

De acuerdo con la página «IAEA Nuclear Security Series», del sitio oficial en inglés del OIEA, la elaboración de las guías de la colección de seguridad nuclear está a cargo de tres grupos de trabajo. En primer lugar, se encuentra la Secretaría del OIEA, la cual está encabezada por el Director General y conformada por profesionales de diferentes campos y países que tienen a su cargo la ejecución de los planes del organismo; entre estos profesionales, se cuenta con expertos nucleares y especialistas e ingenieros en radiación, quienes se encargan de ayudar a los países a cumplir las normas de seguridad internacionales, además de editores, traductores e intérpretes («Secretariat»). En segundo lugar, aparecen los Estados Miembros del OIEA, 168 a febrero del 2016 («Member States»), quienes colaboran con la creación de los borradores de las

[1] En español llamado Organismo Internacional de Energía Atómica (OIEA). En adelante se hará referencia a este organismo por su nombre en español.

publicaciones. Y, por último, se menciona al Comité de Orientación sobre Seguridad Física Nuclear (NSGC, por sus siglas en inglés), el cual, según el *Informe sobre la seguridad física nuclear de 2014*, es «un órgano permanente de altos representantes en la esfera de la seguridad física nuclear, [cuya] finalidad es formular recomendaciones al Director General Adjunto sobre la elaboración y el examen de las publicaciones de la Colección de Seguridad Física Nuclear del OIEA» (8).

El texto original es un texto técnico y normativo que consiste en una guía sobre los contenidos que deberían incluir los reglamentos y procedimientos creados por cada país, autoridad reguladora y operador de fuentes radiactivas en relación con la protección de dichas fuentes. Es necesario señalar que algunos segmentos de esta publicación, particularmente los cuadros, pueden encontrarse en otros documentos elaborados por el OIEA, como el *Código de Conducta sobre seguridad tecnológica y física de las fuentes radiactivas* y otras guías, puesto que cada documento sirve de referencia para los otros. Sin embargo, al todos tener propósitos diferentes, el énfasis de la información proporcionada difiere y, en muchas ocasiones, la terminología queda desactualizada. La falta de una versión oficial en español de esta guía lleva a la decisión de traducir este documento. Por su carácter referencial, esta guía es ampliamente citada en los reglamentos de los diferentes organismos y otras publicaciones del OIEA, pero no se cuenta con una versión en español que garantice la uniformidad terminológica y corrija posibles errores de correspondencia entre los diferentes textos oficiales.

Este proyecto de investigación ofrece la traducción de dicho documento al español y propone estrategias aplicables de documentación para traductores de textos similares. La investigación pretende aplicar un método compuesto por las siguientes estrategias documentales: conocer el contexto dentro del cual se enmarca la guía, reconocer las

características que definen a la guía como texto técnico, identificar necesidades informativas, buscar fuentes documentales en línea que puedan ayudar a solventar tales necesidades, evaluar dichas fuentes y documentar esta evaluación mediante fichas descriptivas.

Justificación

La guía *Security of Radioactive Sources* consta de cuatro capítulos, cuatro apéndices, una sección de referencias y otra de definiciones. De estos, los traducidos para esta investigación son «Introduction», «Responsibilities of the State and Operator, «Security Concepts», «Establishing a Regulatory Programme for Radioactive Source Security», «Definitions» y «References». La razón por la cual se eligieron estas secciones es porque conforman el grueso del contenido que el OIEA espera se incluya en los reglamentos para asegurar la seguridad física de las fuentes radiactivas.

La necesidad de traducir este documento surge a raíz de trabajar con una agencia de traducción en la que una gran parte del volumen de trabajo consiste en textos relacionados con la protección de fuentes radiactivas. Las solicitudes de traducción las realizan normalmente organismos que han reconocido la necesidad de que los países protejan estas fuentes y utilicen las publicaciones del OIEA como referencia para sus marcos normativos. Como ya se mencionó, este documento no ha sido traducido de forma oficial al español; prueba de ello es que su traducción en este idioma no se encuentra disponible en la página oficial del OIEA, donde se ubicaría en caso de existir una versión oficial. Dada su importancia tanto para los Estados como las autoridades reguladoras y las instituciones que gestionan la seguridad física de las fuentes radiactivas, se considera necesario proponer una traducción para los hablantes del español. A pesar de la falta de una traducción oficial, la guía en cuestión es ampliamente citada en capacitaciones y utilizada como documento base por parte de diferentes países y entidades en la

preparación de reglamentos para la protección de fuentes radiactivas. Además, es también citada en otras guías en español publicadas por el OIEA, aun cuando no se cuenta con una versión oficial en español. Por tanto, se considera necesario contar con esta guía de implementación traducida para que esté a disposición de la comunidad hispanohablante.

En los textos oficiales o en las capacitaciones en las que se cita la guía *Security of Radioactive Sources*, los diferentes organismos recurren a una terminología y un estilo que corren el riesgo de no estar estandarizados a falta de un documento oficial en español. A raíz de esto, por un lado, existe el peligro al que pueden estar expuestos los Estados, las personas y el medio ambiente si las fuentes radiactivas fueran mal gestionadas debido a la falta de claridad, falta de correspondencia, o falta de precisión entre la información que se presenta en los diferentes textos que citan a la guía en cuestión. Es esencial que las partes involucradas en la gestión y la protección de fuentes radiactivas cuenten con la documentación necesaria para poder elaborar reglamentos internos que se adecúen a las necesidades y los estándares de contenido tanto nacionales como internacionales. Como resultado de esta realidad, se propone la traducción de esta guía de implementación, la cual espera tener un impacto positivo en la sociedad al colaborar con los esfuerzos por garantizar la seguridad de las fuentes radiactivas. Al contar con un documento en español, los diferentes entes involucrados ahorrarían tiempo y dinero, además de que garantizaría la protección de las fuentes de manera más anticipada.

En el campo traductológico, se pretende que esta investigación se convierta en un modelo útil para la traducción de guías de seguridad de fuentes radiactivas. El uso de estrategias adecuadas de documentación acortaría el tiempo que se emplea en la traducción de documentos cuya función pragmática requiere de gran precisión, como es el caso de esta guía dada su naturaleza normativa. Proponiendo estrategias de documentación, se trazará el camino que

podrían seguir futuros traductores, lo cual redundará en menores tiempos de entrega, aspecto fundamental que deben manejar los traductores. Al respecto, en *Documentación y traducción: Ámbitos de convergencia de dos disciplinas transversales*, bien señalan Merlo Vega y Arroyo Izquierdo lo siguiente:

> La optimización del proceso de documentación es esencial porque responde no sólo a las exigencias de los clientes sino a la propia organización del traductor, que gestionará mejor su tiempo sobre todo en casos en los que tenga que compaginar varios proyectos a la vez en unos plazos de entrega limitados. (15)

A menudo, las solicitudes de traducción requieren plazos de entrega cortos, exigencia que se puede cumplir mediante la aplicación de estrategias adecuadas de documentación sin sacrificar la calidad y la precisión del texto final. Por esta razón, se propone un método que ayude a los traductores a cumplir con los plazos de entrega y los estándares de calidad.

Hasta el momento, en la bibliografía relacionada con la documentación aplicada a la traducción, no se han encontrado estrategias que se puedan aplicar a las guías de seguridad de fuentes radiactivas para solventar los distintos problemas que se puedan presentar en su traducción. Como una respuesta a este vacío, este estudio se centra en la traducción de las guías de seguridad de fuentes radiactivas, en concreto las guías desarrolladas por el OIEA, y la labor documental que dicho proceso conlleva. Si bien las investigaciones traductológicas estudiadas hasta el momento proponen la creación y el uso de herramientas tales como glosarios y bases de datos para mejorar los procesos de documentación, la mayoría se refieren a textos técnicos y científicos en general; hasta la fecha, no se han encontrado referencias específicas al método de documentación aplicable al tipo de texto que interesa en este estudio. Esta investigación intentará llenar ese vacío para que sea aprovechado por traductores de este tipo de guías.

Objetivo general de la investigación

El objetivo general de esta investigación es el siguiente:

Proponer estrategias de documentación adecuadas para la traducción de guías de seguridad de fuentes radiactivas.

Objetivos específicos de la investigación:

Los objetivos específicos son los siguientes:

1. Identificar necesidades informativas terminológicas, temáticas y referenciales de la guía *Security of Radioactive Sources* que puedan ser solventadas mediante estrategias adecuadas de documentación.
2. Proponer estrategias documentales de búsqueda y evaluación de fuentes que puedan ayudar a solventar las necesidades informativas terminológicas, temáticas y referenciales planteadas por la traducción de las guías de seguridad de fuentes radiactivas.

Antecedentes

Como se mencionó anteriormente, el OIEA crea diferentes publicaciones relacionadas con la seguridad de las fuentes radiactivas. En el caso de la Nuclear Security Series, esta se divide en cuatro grandes grupos: Nociones fundamentales de seguridad física nuclear, Recomendaciones, Guías de aplicación y Orientaciones técnicas (*La seguridad física en el transporte de materiales radiactivos* s. pag.). A manera de ilustración, se puede mencionar el documento titulado *La seguridad física en el transporte de materiales radiactivos*. Puesto que el transporte de materiales radiactivos se da en lugares de dominio público, esta guía ofrece medidas para evitar el robo y el sabotaje de fuentes radiactivas durante la transición de un lugar a otro. Para ello, brinda recomendaciones que abarcan los modos de transporte, el tipo de bultos

con los que se trasladan las fuentes, las responsabilidades de los involucrados, entre otras. Otro ejemplo de este tipo de documento es la *Clasificación de fuentes radiactivas*. Esta guía de seguridad presenta el sistema de clasificación de las fuentes con base en su nivel de actividad y el peligro que puedan representar para las personas y el medio ambiente. Estas publicaciones se complementan y sirven de referencia entre ellas. Es pertinente mencionar, además, que la mayoría de estas guías se puede descargar de forma gratuita de las páginas oficiales del OIEA.

En cuanto al tema de la documentación, eje temático de esta investigación, es necesario apuntar que su definición tiende a ser confusa. En «La documentación en la traducción especializada», María José Recoder y Pilar Cid, citando a Babe y a Codina, advierten que el término documentación es ambiguo ya que se puede usar en varios contextos. En el coloquial, se puede utilizar para referirse a documentos impresos (p. ej., «ya recolecté la documentación que me solicitaron»). Como profesión, se puede usar para referirse a las actividades encargadas del diseño y la implementación de sistemas de información y documentación. En su dimensión económica, se utiliza cuando se refiere a entidades relacionadas con la industria de la documentación (creación y mantenimiento de bases de datos). Finalmente, y más apegada a los propósitos de la presente investigación, como disciplina científica se define como la «gestión eficiente del conocimiento social, a fin de ponerlo a disposición de un colectivo de usuarios o de la humanidad en su conjunto, con el objetivo de permitir y facilitar el proceso de obtención de nuevos conocimientos» (74). Dadas las diferentes interpretaciones aquí mencionadas, las autoras explican que los textos que traten la documentación deben dejar en claro desde un inicio el enfoque desde el cual van a abordar el análisis de esta disciplina. De hecho, varios estudios que se han encontrado sobre este tema suelen hacer esta delimitación en sus párrafos introductorios.

Como bien ha sucedido con otras disciplinas, a lo largo de las últimas décadas se ha venido constatando el carácter interdisciplinario de la traducción. María José Recoder y Pilar Cid, en un artículo titulado «Traducción y documentación: cooperar para difundir la información», reconocen que ambas disciplinas cumplen con la función de difundir conocimientos y ponerlos a disposición de las personas. Para poder demostrar su conexión, dedican buena parte del estudio a definir los diferentes tipos y modalidades de traducción, así como el papel que deberían ofrecer los diferentes sistemas de documentación a los traductores. Al final ofrecen una lista de recursos documentales clasificados por categorías que podrían ser de utilidad para los profesionales en traducción. Este texto sirve de introducción al tema de la traducción y la documentación como disciplinas relacionadas, pero no entra en detalles sobre estrategias aplicables a la traducción, por lo que se optó por buscar fuentes que se relacionen más directamente con el tema de la investigación.

En la Maestría en Traducción de la Universidad Nacional de Costa Rica, se han encontrado varios estudios que se centran en la traducción de textos técnicos. Por ejemplo, Ana Lucía Chaves Barquero realizó una investigación sobre la influencia del lector meta en el proceso traductológico, esto con base en la traducción de un manual de usuario para un equipo de espectrometría atómica. En su análisis, la autora describe las características del tipo de texto y del lector meta; posteriormente describe ejemplos de terminología especializada que hubo que adaptar al lector experto para que el texto traducido fuera funcional para los usuarios. Esta investigación, al igual que otras encontradas hasta el momento en el repositorio de la maestría, si bien trata sobre textos técnicos, no aborda el tema de la documentación en el proceso de traducción.

En el caso de la alfabetización informacional, Pilar Cid y Remei Perpinyá escribieron un artículo titulado «Competencia informacional en traducción: análisis de los hábitos de los estudiantes universitarios en la consulta y uso de fuentes de información». En dicho artículo se estudiaron los recursos documentales a los que recurrieron estudiantes de traducción para resolver los problemas que se les presentaban al traducir determinados textos. El propósito era conocer los criterios que utilizaban los estudiantes para elegir las fuentes. Los criterios, en orden de preferencia, fueron los siguientes: «recomendación de un profesor, (…) gratuidad de la fuente, la facilidad de acceso y su disponibilidad en línea» (s. pag.). Puesto que este artículo brinda información sobre el proceso documental y la selección de fuentes en el estudio de una población específica, podría servir de referencia para señalar otros usos puntuales de la documentación, en este caso, desde el punto de vista académico.

En otra área de aplicación para la documentación y la traducción, Miguel Ibáñez Rodríguez, de la Universidad de Valladolid, realizó una investigación cuyos resultados publicó en un artículo titulado «La documentación en traducción especializada: el caso de la vitivinicultura». En su investigación, proporciona información relevante sobre la documentación y cómo aplicarla al área de la traducción. Con base en este conocimiento, brinda recursos tanto terminológicos como temáticos que son de utilidad para el traductor de textos relacionados con el vino. Para cada uno de esos recursos, ofrece una pequeña descripción que ayudará a futuros traductores a decidir acerca de la utilidad de los mismos para su trabajo. Este es uno de los pocos estudios que se han encontrado hasta el momento sobre la documentación aplicada a la traducción en un área técnica específica.

Mapa del trabajo de investigación

Este trabajo está dividido en 4 apartados: primer capítulo, segundo capítulo, tercer capítulo y conclusiones. El primer capítulo es el aparato crítico sobre el que se basa esta investigación, el cual está dividido en marco teórico y marco metodológico: en el marco teórico se detallan conceptos y teoría sobre la documentación y su uso en la traducción de textos técnicos; en el marco metodológico se explican las estrategias de documentación que se utilizaron en este trabajo para crear un método documental aplicable a la traducción de la guía *Security of Radioactive Sources*. El segundo capítulo de esta investigación, se describe el contexto dentro del cual se enmarca la guía en estudio, define las características de la guía que la identifican como texto técnico y presenta ejemplos de las diferentes necesidades informativas terminológicas, temáticas y referenciales que se identificaron como parte del proceso de documentación. En el tercer capítulo, se detallan las estrategias documentales utilizadas para solventar las necesidades informativas planteadas en el primer capítulo y se exponen algunos ejemplos para ilustrar el proceso llevado a cabo.

Capítulo 1: Marco teórico y metodológico del uso de técnicas de documentación aplicables a la traducción de la guía *Security of Radioactive Sources*

1.1. Introducción

En este apartado se expone la base teórica y metodológica sobre la cual se apoyará la presente investigación. En el marco teórico, en primer lugar, se presentarán las características de los textos de tipo técnico según la bibliografía encontrada; además, se incluirán las particularidades de la traducción de este tipo de textos. En segundo lugar, se definirá el concepto de documentación y su relación con el campo de la traducción como disciplina práctica. En tercer lugar, se expondrán estrategias de documentación aplicables al campo de la traducción. En el marco metodológico, se partirá de la base teórica para explicar el análisis que se llevará a cabo en el presente estudio con el propósito de cumplir con los objetivos del mismo.

1.2. Marco teórico

El objeto de este estudio es la traducción de la guía *Security of Radioactive Sources*, la cual se considera un texto técnico. En general, se tiende a considerar que los textos técnicos y científicos comparten las mismas características; sin embargo, Jody Byrne los distingue a cada uno como textos con características propias. En el capítulo titulado «Scientific and Technical Translation», Byrne expone las particularidades de los textos especializados para que traductores o formadores de traductores puedan desarrollar un sentido crítico que los ayude a tomar mejores decisiones en la práctica de la traducción. Apoyado en ideas de David Locke, Byrne explica que los textos científicos tienden a tener un grado mayor de estilo propio y creatividad en comparación con los textos técnicos, pues se espera que los primeros tengan un carácter más innovador. En cambio, los textos técnicos parten del conocimiento científico ya establecido para ponerlo en práctica en un área en particular (3). Esta distinción se considera

importante ya que la manera más directa en la que los textos técnicos presentan la información es parte de los aspectos a considerar al tomar decisiones relacionadas con su traducción.

Para poder definir más detalladamente las características de los textos de tipo técnico, este estudio toma como base la propuesta de Kenneth Budinski. En «What is Technical Writing», Budinski lista características generales de los textos técnicos para la American Society for Metals International, la cual reúne a expertos en ciencias de materiales e ingeniería. Esta obra está dirigida a expertos de distintas disciplinas técnicas que requieren crear textos para colegas dentro de sus áreas de conocimiento; la intención de Budinski es que los autores se familiaricen con las características de los textos técnicos para que sus obras se adapten a lo que el público meta espera. Budinski plantea los siguientes rasgos del texto técnico:

1. It pertains to a technical subject.
2. It has a purpose.
3. It has an objective.
4. It conveys information/facts/data.
5. It is impersonal.
6. It is concise.
7. It is directed.
8. It is performed with a particular style and in a particular format.
9. It is archival.
10. It cites contributions of others. (4)

El autor sugiere que si bien estas características no son las únicas, son algunas de las más importantes para distinguir este tipo de texto. Cada uno de estos aspectos podría acarrear

problemas traductológicos que requieran estrategias concretas para su solución, dada la fidelidad con la cual se espera llevar a cabo la traducción de estos documentos.

Desde la perspectiva del traductor, conocer las características del tipo de texto podría ayudar a identificar problemas traductológicos desde un inicio o, al menos, servir de guía para identificar aspectos a los que se debe poner especial atención en las diferentes fases de la traducción. En la obra citada en párrafos anteriores, Byrne también distingue la traducción técnica y la traducción científica de la siguiente manera:

> While a technical text is designed to convey information as clearly and effectively as possible, a scientific text will discuss, analyze and synthesize information with a view to explaining ideas, proposing new theories or evaluating methods. Due to these differing aims, the language used in each type of text, and consequently the strategies needed to translate them, may vary significantly. (2)

Esta distinción se considera valiosa puesto que insta a los traductores a estar conscientes de las diferencias entre los textos técnicos y los científicos para poder abordarlos de la mejor manera en el proceso de traducción. Por esta razón, en esta investigación se explorarán las características de la guía en estudio y se indicarán problemas traductológicos cuya resolución se logre mediante técnicas concretas de documentación.

Tal y como se mencionó en la introducción de este trabajo, el objeto de estudio de esta investigación es el proceso de traducción desde la problemática de la documentación. Por esta razón, es necesario elucidar la relación que existe entre ambas disciplinas: la traducción y la documentación. En el artículo «La documentación en la traducción especializada», María José Recoder y Pilar Cid se refieren a la labor documentalista que llevan a cabo los traductores y los recursos a los cuales pueden recurrir. Ellas definen la documentación como una disciplina

científica que tiene como propósito la «gestión eficiente del conocimiento social, a fin de ponerlo a disposición de un colectivo de usuarios o de la humanidad en su conjunto, con el objetivo de permitir y facilitar el proceso de obtención de nuevos conocimientos» (Codina citado por Recoder y Cid 74). Desde la traductología, se puede entender a los traductores como «el colectivo de usuarios» que busca ese conocimiento social para resolver problemas traductológicos mediante la documentación.

A raíz de lo mencionado en el párrafo anterior, la labor documentalista del traductor podría analizarse, a su vez, desde dos vertientes, como lo hace ver Isadore Pinchuck. Esta autora explica que la traducción técnica y científica «is part of the process of disseminating information on an international scale, which is indispensable for the functioning of our modern society» (Pinchuck citada por Byrne 1). Si se analiza esta idea a la luz de lo planteado por Codina, en Recoder y Cid, es posible notar cómo la documentación permea la labor traductológica en momentos diferentes del proceso de traducción. Por un lado, la documentación funciona como herramienta para resolver problemas traductológicos; y, por otro lado, las traducciones también ponen a disposición un conocimiento en particular a otros colectivos hablantes de otras lenguas.

Aunque varios autores plantean que es necesario que los traductores puedan encontrar y evaluar la calidad de los recursos disponibles, en la bibliografía consultada hasta el momento, ninguno detalla estrategias de documentación que sean aplicables a la presente investigación. Para los propósitos de este estudio, las estrategias documentales se definirán como las técnicas empleadas para el análisis, la clasificación y la evaluación de los problemas de traducción y de los recursos documentales aplicables a la tarea traductora. En adelante se presentarán distintas estrategias descritas por diferentes autores que se podrían utilizar en la traducción de guías de seguridad de fuentes radiactivas.

Varias obras consultadas coinciden en que la documentación, como disciplina de apoyo, forma parte de diferentes etapas de la traducción, las cuales es preciso identificar. Para efectos de esta investigación, se considera relevante la distinción hecha por José Antonio Merlo Vega, quien introduce el curso de «Documentación aplicada a la traducción»[2] detallando las etapas traductológicas de las que forma parte la documentación. Según este autor, el proceso de traducción cuenta con dos etapas: la primera se conoce como el proceso semasiológico y la segunda como el proceso onomasiológico. La fase semasiológica consiste en la búsqueda de recursos que ayuden a entender la temática del texto original, mientras que la fase onomasiológica comprende la recolección de herramientas que puedan solventar las necesidades terminológicas y fraseológicas que surgen al traducir (4). Distinguir estas dos fases es importante pues en cada una de ellas surgen problemas traductológicos diferentes. En el caso de los textos técnicos, se podría entender que en el proceso semasiológico aparecen problemas relacionados con el entendimiento del texto, en particular del área de conocimiento que se desarrolle; en el proceso semasiológico surgen más bien problemas que involucran el cómo transmitir ese conocimiento de la manera más precisa y adecuada a los usuarios del texto traducido. Como se verá a continuación, la bibliografía encontrada propone diferentes estrategias documentales para ayudar a resolver los problemas que surgen en ambas fases del proceso de traducción.

Como punto de partida para la selección de estrategias de documentación aplicables a la traducción, se siguieron las recomendaciones de María José Recoder y Pilar Cid en «La

[2] Si bien esta fuente no cuenta con sello editorial y solo forma parte de los programas de los cursos impartidos en la Universidad de Salamanca, se tomó en consideración el papel de Merlo Vega como autoridad en el tema. Además, se buscaron otros documentos de este autor que brindaran la información aquí presentada sin resultados positivos, por lo que se decidió incluir esta fuente por su relevancia para el presente trabajo.

documentación en la traducción especializada». Las autoras proponen que los traductores evalúen los siguientes cuatro aspectos antes de iniciar la búsqueda de fuentes documentales:

1. El problema de traducción para saber qué hay que buscar
2. La accesibilidad que se tenga de las fuentes documentales
3. El tiempo con el que se cuente para la recopilación y evaluación de las fuentes
4. El conocimiento del traductor en materia de sistemas de búsqueda (Recoder y Cid 79)

El manejo de los sistemas de búsqueda es especialmente necesario cuando la solicitud de traducción implica un tema nuevo o desconocido; sin embargo, se convierte en una habilidad fundamental cuando se prefiere usar sistemas informáticos para la recopilación de fuentes. Este aspecto se relaciona con la accesibilidad, pues la búsqueda de las fuentes también mostrará cuán accesible es un documento en particular relacionado con el texto por traducir; y, tanto para temas nuevos como para los previamente investigados, el tiempo dedicado al proceso de traducción se podría aprovechar mejor si se cuenta con estrategias para la recopilación y la evaluación de fuentes. El problema de traducción es el enfoque principal que se tomará en este proyecto, ya que de aquí se derivan las necesidades traductológicas del documento, que a su vez darán las pautas para la selección de los recursos documentales que puedan cubrirlas.

La traducción de la guía *Security of Radioactive Sources* lanzó varios problemas de traducción que serán clasificados a partir de la tipología propuesta por José Antonio Merlo Vega y Sonia Arroyo Izquierdo. En «Documentación y traducción: ámbitos de convergencia de dos disciplinas transversales», estos autores detallan la manera en que se puede emplear la documentación para solventar problemas en el proceso de traducción. Al referirse a estos problemas, los autores utilizan el término «necesidades de información» (126) y las clasifican de la siguiente manera:

1. Necesidades informativas terminológicas: se refieren a palabras, en particular aquellas de las cuales se desconozca el significado. Estas se deberían poder resolver con herramientas básicas como diccionarios.

2. Necesidades informativas fraseológicas: se refieren a las unidades de sentido formadas por más de una palabra las cuales destacan por su nivel de especialización.

3. Necesidades informativas temáticas: se refieren al contenido del texto y la materia que aborda. Son importantes porque son la base del entendimiento del texto, previo a la fase de traducción.

4. Necesidades informativas culturales: se refieren a nombres de las empresas, instituciones o particulares que elaboran el texto y cuya equivalencia en el texto traducido podría no estar clara.

5. Necesidades informativas contextuales: se refieren a las dudas que se tengan sobre el objetivo que cumpliría la traducción para el público meta. Estas indicarían el grado de adaptación que pueda requerir el texto traducido sin que se pierda el sentido original.

6. Necesidades informativas profesionales: se refiere a la responsabilidad legal como traductores. (Merlo Vega y Arroyo Izquierdo 20-21)

Los autores señalan que estas necesidades tendrán diferentes prioridades dependiendo del tipo de texto y la situación traductológica. Además, destacan que existen diferentes recursos para solventar cada una de ellas, los cuales es preciso saber evaluar.

Este estudio girará en torno a las necesidades terminológicas y temáticas de una traducción, con base en la clasificación de Merlo Vega y Arroyo Izquierdo. Dado que una de las características de los textos técnicos es la precisión, identificar estas necesidades será una etapa fundamental del proceso documental, pues se contará con un registro de problemas que

deberán ser solventados mediante otras técnicas de documentación. Sin embargo, como menciona Budinski, ya que el texto técnico contiene referencias a otros documentos (4), el proceso de traducción a una segunda lengua suele plantear necesidades referenciales, una categoría que se decidió agregar a la lista de problemas por solventar. Las referencias a otros textos pueden acarrear problemas de traducción como los que se listan a continuación:

- El título puede hacer referencia a una fuente bibliográfica que haya sido actualizada, por lo que el traductor valorará cuál versión incluir en la lista de referencias.
- La referencia puede ser a un texto no traducido al español. En este caso, el traductor podría decidir entre dejar el título en inglés u ofrecer una traducción *ad hoc* en español del título para que el lector meta tenga una idea de qué trata dicho texto.

Consideraciones similares a estas llevaron a incluir el problema de las referencias como otra necesidad informativa. Se consideró que técnicas adecuadas de documentación podrían ayudar a solventar estas necesidades de manera eficaz.

Para la selección de los recursos que se utilizarán en la solución de los problemas traductológicos, este trabajo toma como punto de partida lo que se expone en «Competencia informacional para la actividad traductora». En este artículo, Eva Ortoll Espinet propone ciertas habilidades que debería desarrollar el traductor para abordar los retos que surjan en el proceso de traducción. La autora considera que para poder solventar las complicaciones, convendría que los traductores aplicaran «estrategias que permitan encontrar la información necesaria, lo que implica el conocimiento y la utilización de recursos de información, así como valorar su utilidad, fiabilidad y calidad» (s. pag.). Según este planteamiento, la labor documentalista del traductor debería incluir la búsqueda de fuentes documentales y su correspondiente evaluación. Dicha

destreza se conoce como competencia informacional o alfabetización informacional, tema que se abordará más adelante.

Los procesos de documentación aplicados a la traducción suelen ser analizados desde distintas perspectivas. Para la presente investigación, se optará por seguir las etapas de búsquedas propuestas por Merlo Vega en «Uso de la documentación en el proceso de traducción especializada». Este autor propone seguir el siguiente orden:

1. Búsqueda de recursos sobre la lengua
2. Búsqueda de recursos sobre la terminología especializada
3. Búsqueda de información sobre la materia
4. Búsqueda de textos paralelos
5. Búsqueda de especialistas (330)

Las búsquedas de recursos sobre la lengua abarcan la aclaración de dudas relacionadas con vocabulario general, gramática, sintaxis y morfología, mientras que las búsquedas de recursos sobre la terminología especializada se centrarán en el vocabulario técnico o especializado. Mediante las búsquedas de información sobre la materia, de textos paralelos y de especialistas se intenta resolver dudas relacionadas con el área de conocimiento o sobre el contenido del texto. El orden propuesto por Merlo Vega brinda pautas que se pueden seguir para formular un método de documentación, por lo que para cumplir con los objetivos del presente trabajo, se van a explorar las búsquedas de recursos sobre terminología especializada, las búsquedas de información sobre la materia y las búsquedas de textos paralelos.

Como se mencionó anteriormente, la resolución de los problemas traductológicos mediante la documentación supone la búsqueda y la evaluación de recursos documentales. Derivado de esta situación y acuñado desde el área de la bibliotecología, surgió el término

«alfabetización informacional». Varios autores citan la definición que se encuentra en el «Presidential Committee on Information Literacy: Final Report», en el cual la Association of College & Research Libraries define alfabetización informacional como la capacidad para «recognize when information is needed and have the ability to locate, evaluate, and use effectively the needed information» (s. pag.). Esta definición destaca que el propósito de localizar, evaluar y usar las fuentes documentales es solventar adecuadamente las necesidades de información, las cuales es preciso haber identificado previamente.

Para abordar la relevancia de la alfabetización informacional dentro del tema de la documentación aplicada a la traducción, este trabajo toma como referencia el documento titulado «Documentación y traducción: Ámbitos de convergencia de dos disciplinas transversales», en el cual Merlo Vega y Arroyo Izquierdo indican que los traductores pueden desarrollar la capacidad para resolver por sí mismos problemas traductológicos de la manera más precisa, pero que para ello es necesario que desarrollen su sentido crítico y «métodos que faciliten la búsqueda de datos en el futuro» (122). El sentido crítico es posible que sea resultado de la formación, la experiencia o la retroalimentación recibida. Sin embargo, las estrategias para facilitar la búsqueda de datos en futuras tareas traductoras son parte de lo que busca explorar este trabajo a partir de la teoría sobre la documentación aplicada a la traducción. En última instancia, estas estrategias también podrían ayudar a desarrollar el sentido crítico al cual se refieren los autores.

En la propuesta de estrategias de documentación aplicables a la traducción en su etapa onomasiológica, el énfasis del presente trabajo será la evaluación de fuentes electrónicas. Esta investigación toma los criterios de evaluación de lo expuesto por María Pinto, quien ha escrito diferentes artículos relacionados con la documentación aplicada a la traducción y es citada por

varios autores que desarrollan este mismo tema. En «Calidad y evaluación de los contenidos electrónicos», Pinto presenta una serie de parámetros generales que se pueden utilizar para evaluar los recursos que se encuentren en la web; dentro de cada parámetro, se incluyen diferentes criterios que ayudan a determinar si el parámetro se cumple al menos de manera parcial. A continuación se presentan los diferentes parámetros propuestos por Pinto:

1. Autoría: en este parámetro se evalúa al responsable de los contenidos de un sitio web. Sea una persona o una organización, debe estar claramente identificado. Se podría incluir también la declaración de objetivos o finalidad del sitio web con base en las intenciones del autor.
2. Actualización y actualidad: se evalúa cuán actualizados están los contenidos del sitio web. Se debería buscar la fecha de creación y actualización de los contenidos, la presencia de información actual y actualizada, la existencia de enlaces obsoletos o erróneos.
3. Contenido: este parámetro evalúa la información que proporcione el sitio web, aunque Pinto aclara que este punto tiende a ser subjetivo. Se considera, por ejemplo, elementos como la exactitud, la precisión, el rigor, la pertinencia y la objetividad del contenido.
4. Accesibilidad: Evalúa las dificultades y limitaciones con las que puede encontrarse un usuario y que podrían potencialmente hacer que el sitio no sea accesible por todas las personas. Por ejemplo, en este apartado se podría incluir la necesidad de instalar *plugins* adicionales para el adecuado funcionamiento del sitio web, la posibilidad de imprimir y visualizar correctamente la impresión de los contenidos del sitio o la existencia de un menú de ayuda al usuario.
5. Funcionalidad: evalúa la facilidad con que un usuario puede localizar la información que requiere. En este parámetro están incluidos criterios relacionados con la estructura y organización de los contenidos la pertinencia y adecuación de los títulos, la existencia de un mapa web y la existencia de un sistema de búsqueda de contenidos propios.

6. Navegabilidad: La navegabilidad se refiere a la facilidad para desplazarse a las diferentes páginas que componen un sitio web. Para esto, se consideran criterios como la presencia de un menú de contenidos visible y funcional y la presencia de botones de navegación.

7. Diseño: evalúa el aspecto físico y la ergonomía del sitio web. Los criterios de evaluación incluyen la adecuada combinación de colores, formas e imágenes, la tipografía adecuada y la homogeneidad de estilo y formato en todas las páginas del sitio web. (s. pág.)

Como parte del proceso documental, esta investigación propone una forma de organización de las fuentes documentales para su respectiva evaluación. En *Selección y evaluación de recursos lingüísticos en internet para el traductor especializado*, Consuelo Gonzalo García y Esther Fraile Vicente proponen crear fichas descriptivas para cada recurso documental a partir de una metodología predeterminada, lo cual facilitaría la evaluación de las fuentes documentales durante el proceso de traducción o en futuras traducciones. Para que tales fichas cumplan su función, las autoras plantean que el traductor, en su labor documentalista, defina previamente los siguientes conceptos:

1. Parámetros: características o aspectos genéricos del recurso digital que será evaluado.
2. Indicadores: aspectos o elementos del recurso digital que tendremos en cuenta para medir la operatividad de un parámetro.
3. Procedimientos: método elegido para poder aplicar criterios de calidad a un recurso, es decir, parámetros e indicadores seleccionados con anterioridad. (339)

Como se puede apreciar, estos conceptos mantienen cierta similitud con las ideas de Pinto. Sin embargo, Gonzalo García y Fraile Vicente van más allá y proponen un modelo de ficha con base en parámetros establecidos por ellas, lo cuales también podría ser utilizadas por un traductor en la evaluación de sus fuentes documentales. Por ejemplo, se incluyen parámetros

como el llamado «descriptores» para incluir términos genéricos relacionados con el área de estudio del recurso documental, y «evaluación» para asignar al documento consultado una evaluación del 1 al 5 en cuanto a calidad con base en los parámetros anteriores (334). En la presente investigación, estas fichas servirán de modelo para crear fichas descriptivas propias con base en los parámetros y criterios de evaluación propuestos por Pinto.

1.3. Marco metodológico

Con el propósito de cumplir con los objetivos de este trabajo, se propone un método documental que se basa en la teoría sobre estrategias de documentación aplicables a la traducción de guías de seguridad de fuentes radiactivas. Uno de los primeros pasos de este proceso será conocer el sistema de publicaciones del Organismo Internacional de Energía Atómica, incluidos los tipos de documentos que redactan y publican, cómo se organizan, distribuyen y clasifican. El propósito de esto es conocer el marco dentro del cual se ubica la guía *Security of Radioactive Sources* y familiarizarse con sus contenidos y características terminológicas. Como ya se mencionó en la presentación general de esta investigación, la página «IAEA Nuclear Security Series», la cual ofrece información acerca de las características generales de las guías para la protección de fuentes radiactivas, explica que las publicaciones son redactadas y revisadas por la Secretaría del OIEA, los Estados Miembros del OIEA y el Comité de Orientación sobre Seguridad Física Nuclear (NSGC, por sus siglas en inglés). Contando con esta información, se pretende investigar más a fondo cuáles recursos documentales se emplean en la elaboración de los borradores de las publicaciones del OIEA y cómo se realiza la revisión y la evaluación del contenido plasmado en los textos.

Una vez entendido el proceso que se empleó en la creación del texto original, el siguiente paso es reconocer las características de la guía como texto técnico con base en lo expuesto por

Kenneth Budinski; esto con el propósito de dilucidar con anticipación los posibles retos que supone la traducción de la guía *Security of Radioactive Sources*. A continuación, se procede a identificar y analizar los retos traductológicos que presenta la traducción de la guía. Para lograrlo, con base en las recomendaciones de Merlo Vega y Arroyo Izquierdo, esta investigación presentará ejemplos de necesidades informativas terminológicas, temáticas y referenciales que surgieron a partir de la traducción de la guía en estudio. Se eligieron estas tres porque se consideró que eran las que más aplicaban a la traducción del texto y a los propósitos de esta investigación en materia de traductología y documentación. Se dedicará una sección del segundo capítulo a detallar ejemplos de cada una de las necesidades informativas ya mencionadas, los cuales se originan a partir de los problemas más recurrentes en la traducción de la guía en estudio.

Identificadas las necesidades, en la siguiente etapa se procederá a recolectar recursos documentales y a evaluar la capacidad de las fuentes documentales para solventar los problemas traductológicos identificados. Con el propósito de ilustrar el proceso que llevaría a cabo un traductor y establecer los límites del alcance de la investigación, se emplearon únicamente fuentes electrónicas. Para la fase de recolección, se seguirán las recomendaciones de Merlo Vega en relación con el orden de las búsquedas de recursos documentales. Se consideró que las que podrían mostrar de manera más clara el proceso de documentación basado en fuentes electrónicas serían las siguientes:

a. Búsquedas sobre terminología especializada: se utilizó el motor de búsqueda de Google para encontrar diccionarios o glosarios monolingües que ayudaran a aclarar dudas terminológicas planteadas en el segundo capítulo de la investigación. Para esto, se emplearon términos específicos de búsqueda que serán ilustrados en el desarrollo del tercer capítulo. Se

añadirán capturas de pantalla de los resultados y se analizarán y evaluarán los primeros dos resultados de cada búsqueda específica.

b. Búsquedas de información sobre la materia: se utilizó el motor de búsqueda de Google para encontrar recursos documentales que ayudaran a resolver las necesidades temáticas planteadas en el segundo capítulo de la investigación. Para esto, se emplearon términos específicos de búsqueda que serán detallados en el tercer capítulo. Se añadirán capturas de pantalla de los resultados y se analizarán y evaluarán los primeros dos resultados de cada búsqueda específica.

c. Búsqueda de textos paralelos: por medio de la página «IAEA Nuclear Security Series», se buscaron publicaciones que contaran con versión en inglés y español. Puesto que dentro de esta colección existen cuatro categorías de publicaciones, se analizó la versión más reciente de cada categoría. Se consideró que la elección de estos textos sería la más realista para analizar la utilidad de los textos paralelos en las publicaciones que pertenecieran a la Colección de Seguridad Física Nuclear del OIEA, tal como la guía en estudio.

En las fases iniciales de este trabajo, se incluyó la búsqueda de recursos sobre la lengua. Sin embargo, se descubrió que los resultados eran muy amplios y aportaban poco a la resolución de las necesidades particulares, lo que causaba que su análisis se volviera redundante y poco provechoso. La búsqueda de especialistas se obvió puesto que no concordaba con el enfoque de este trabajo que era el uso exclusivo de fuentes electrónicas.

Como parte de las estrategias de documentación propuestas y con base en la recomendación de Gonzalo García y Fraile Vicente, se crearon además fichas descriptivas para la evaluación de las fuentes documentales y como registro de las fuentes consultadas, las cuales

se pueden encontrar en los Anexo 2-18. El modelo de ficha se puede observar en la siguiente imagen:

Imagen 1. Modelo de ficha descriptiva.

Datos del documento o página web		
Nombre del archivo o página web		
Dirección URL de visita o descarga		
Fecha de consulta		
Idioma		
Breve descripción del contenido		
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido		☐
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización		☐
Gramática y vocabulario aceptables		☐
Afinidad con el TO		☐
Compatibilidad		
Formato funcional		☐
Versiones en otras lenguas		☐
Funcionalidad y navegabilidad		
Estructura y organización lógicas		☐
Menú/marcadores de contenido funcionales		☐
Diseño		
Diseño funcional		☐
Adecuada combinación de colores y formas		☐
Tipografía adecuada		☐
Pertinencia		
Necesidades informativas terminológicas ☐	Necesidades informativas temáticas ☐	Necesidades informativas referenciales ☐

Los parámetros y criterios elegidos fueron adaptados a partir de las recomendaciones hechas por María Pinto para la evaluación de fuentes electrónicas. En la primera sección de la ficha se encontrará información básica sobre la fuente con el propósito de que sea fácil ubicarla en un futuro, en caso de ser necesario. Esta sección incluirá información sobre el nombre del documento (en algunos casos se encontraban en formato PDF) o página web, su enlace, la fecha de consulta, el idioma y una breve reseña del contenido. Las siguientes secciones de la ficha incluyen diferentes parámetros con sus respectivos criterios de evaluación; para cada criterio,

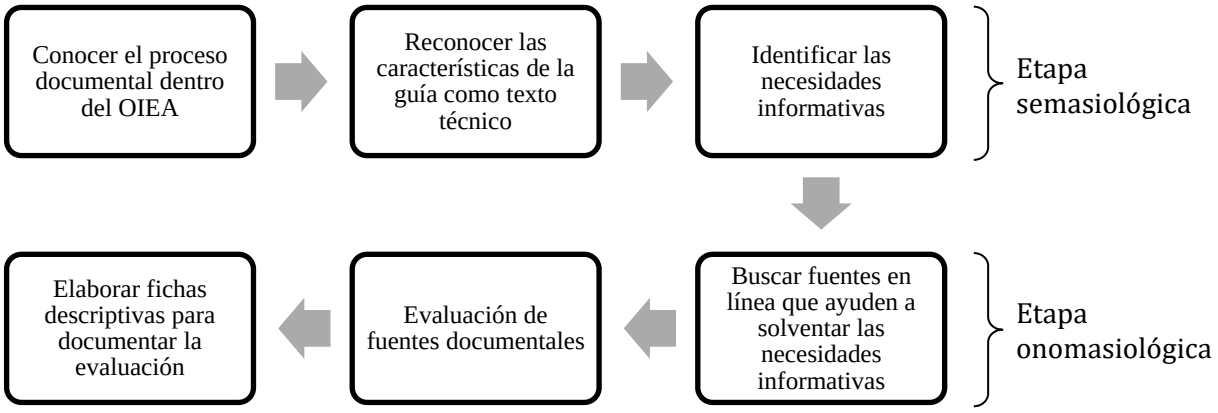
se agregaron casillas de verificación y comentarios para indicar si el criterio se cumplía o no. Los parámetros y los criterios elegidos fueron los siguientes:

a. Contenido y uso del lenguaje
    i. Fecha de creación y actualización
    ii. Breve descripción del contenido
    iii. Gramática y vocabulario aceptables
    iv. Afinidad con el texto original (TO)
b. Compatibilidad
    i. Formato funcional
    ii. Versiones en otras lenguas
c. Funcionalidad y navegabilidad
    i. Estructura y organización lógicas
    ii. Menú/marcadores de contenido funcionales
d. Diseño
    i. Diseño funcional
    ii. Adecuada combinación de colores y formas
    iii. Tipografía adecuada
e. Pertinencia
    i. Necesidades terminológicas
    ii. Necesidades temáticas
    iii. Necesidades referenciales

Cabe aclarar que, para el parámetro de pertinencia, se consideraron como criterios la capacidad del recurso documental para resolver las necesidades informativas planteadas en el segundo capítulo de esta investigación.

A continuación se muestra un flujo de trabajo que ilustra el modelo de proceso documental desarrollado para esta investigación y que resume la metodología presentada en esta sección del trabajo:

Imagen 2. Flujo de trabajo del proceso de documentación propuesto para la traducción de la guía *Security of Radioactive Sources*.



1.4. Conclusión

Se considera que si bien la base teórica utilizada en este trabajo muestra distintos alcances, algunos de los cuales no remiten a la tarea traductora en sí, sirvió para entender el papel de la documentación desde su definición más general hasta su aplicación en un campo como la traducción. Las diferentes técnicas propuestas en varios estudios hicieron posible establecer estrategias de documentación aplicables a la traducción de la guía *Security of Radioactiuve Sources*, las cuales se verán reflejadas en los capítulos de desarrollo de esta investigación.

Capítulo 2 – Etapa semasiológica para la traducción de la guía *Security of Radioactive Sources*: Sistema de publicaciones del OIEA, características de la guía como texto técnico e identificación de necesidades informativas

2.1. Introducción

En este segundo capítulo se brindan detalles sobre las estrategias de documentación aplicadas a la traducción de un texto técnico. En concreto, el apartado presenta las etapas que forman parte del proceso semasiológico de una traducción. Por lo tanto, como primer paso, se hará una reseña sobre el contexto en el cual se enmarca el texto en estudio. Para esto, se hablará sobre el tipo de publicaciones desarrolladas por el Organismo Internacional de Energía Atómica (en adelante llamado OIEA), así como su creación y difusión. Como segundo paso, se analizarán las características del texto original como texto técnico. Contando con esta información, en el tercer paso del método propuesto se procederá a identificar y analizar ejemplos de necesidades terminológicas, temáticas y referenciales del texto en estudio, en particular, las más recurrentes en el proceso de traducción. Uno de los propósitos de esta investigación es recrear el proceso que podrían realizar los traductores al enfrentarse a un nuevo texto. Al finalizar este capítulo, se contará con los elementos necesarios para desarrollar la siguiente parte de esta investigación, la cual buscará solventar las necesidades informativas mediante el uso de otras estrategias de documentación.

2.2. Sistema de publicaciones del OIEA

La primera estrategia de documentación aplicada a la traducción que se propone en este trabajo es buscar información sobre el contexto dentro del cual se elaboró el texto original. Citado por Recoder y Cid, Lluis Codina afirma que la documentación se relaciona con la «gestión eficiente del conocimiento social» (74). Por lo tanto, esta fase brinda al traductor una

vista general del contexto social donde se desarrolla el conocimiento que pretende difundir el texto en estudio. Este paso, a su vez, puede guiar al traductor a encontrar fuentes que le sean útiles en el proceso onomasiológico de la traducción.

Como se puede observar en la página en inglés titulada «Scientific and Technical Publications» del OIEA, este organismo produce diferentes tipos de publicaciones, como por ejemplo, informes técnicos, colecciones de seguridad, normas, manuales de capacitación, entre otros (s. pag.). Cabe mencionar que las páginas oficiales del OIEA, en las cuales se encuentran estos documentos, están en inglés y sus versiones originales suelen estar escritas en ese idioma. Desde la página oficial de este organismo, o mediante una búsqueda simple con un motor de búsqueda en internet, es fácil encontrar estos documentos.

En el caso de la guía *Security of Radioactive Sources*, esta se puede descargar desde la página titulada «Nuclear Security Series Publications». En ella se encuentran las diferentes colecciones con su respectivo número, título, idiomas disponibles y fechas de publicación. La mayoría cuenta con un enlace desde el cual se puede acceder a la versión PDF. En la página «IAEA Nuclear Security Series», se explica que estas colecciones abordan temas relacionados con la «prevention and detection of, and response to, theft, sabotage, unauthorized access and illegal transfer or other malicious acts involving nuclear material and other radioactive substances and their associated facilities». Además, estas colecciones complementan otros tratados y acuerdos que abordan los mismos temas (s. pag.). En la misma página se indica que existen cuatro categorías de estas colecciones, divididas de la siguiente manera: Nuclear Security Fundamentals, Nuclear Security Recommendations, Implementing Guides y Technical Guidance (s. pag.). La oferta de información que contiene el sitio es de gran utilidad no solo para los organismos o instituciones encargadas de crear los reglamentos para el manejo y la

protección de fuentes radiactivas, sino también para futuros traductores de dichos documentos o de temas relacionados con la seguridad radiactiva.

El proceso de elaboración de borradores para estas colecciones se explica muy brevemente en la página «IAEA Nuclear Security Series». Como se mencionó al inicio de esta investigación, en la sección titulada «Drafting and Review» se explica que este proceso lo llevan a cabo la Secretaría del OIEA, los Estados Miembros del OIEA y el Comité de Orientación sobre Seguridad Física Nuclear (NSGC, por sus siglas en inglés). La Secretaría y los Estados Miembros son los encargados de crear los primeros borradores y el NSGC los revisa y aprueba. Una vez que se tienen los borradores, se envían a los Estados Miembros por un período de 120 días para que realicen una revisión formal. Además, desde la página «Forthcoming IAEA Nuclear Security Series Publications», cualquier persona o entidad puede descargar los borradores que entran en esta fase y enviar comentarios antes de la fecha límite indicada al final del listado de publicaciones en etapa de revisión.

En cuanto al desarrollo del contenido, las páginas oficiales del OIEA ofrecen muy poca información. Se indica que se realizan reuniones para que especialistas de los Estados Miembros y de organismos internacionales revisen y discutan lo incluido en los borradores. En uno de los enlaces de esta página, titulado «Review Committees», se encuentra una lista de las próximas reuniones. Además, se señala que en la redacción de estos textos se toman en cuenta los estándares de seguridad radiológica y las actividades de salvaguardia del OIEA. Sin embargo, aparte de lo que se menciona en estas líneas anteriores, es poco lo que se ha encontrado hasta el momento en relación con la elaboración de estos borradores, salvo su carácter técnico y su relación con asuntos de seguridad que involucren a fuentes radiactivas.

2.3. Características de la guía *Security of Radioactive Sources* como texto técnico

Como parte de las estrategias de documentación que se proponen en este trabajo, en esta sección se identifican las características de la guía en estudio como texto técnico. El contexto del cual se desprende el texto original arroja ideas sobre el tipo de documento con el cual se está tratando. Además, sabiendo que esta guía aborda la protección de las fuentes radiactivas, se puede asumir que se está lidiando con un texto especializado y técnico. Este apartado toma como base la lista creada por Kenneth Budinski en «What is Technical Writing» para comprobar que la guía *Security of Radioactive Sources* es un texto técnico. Este análisis también dará luz sobre el tipo de problemas que se deberán enfrentar en la fase de traducción y que se intentarán resolver mediante la documentación.

En cuanto al contenido de la guía, el texto en estudio desarrolla temas relacionados con fuentes radiactivas, sistemas de seguridad, niveles de seguridad, entre otros, los cuales representan necesidades temáticas que se abordarán en secciones posteriores a este capítulo. Todos estos temas están relacionados con un área técnica que requiere cierto conocimiento especializado: la radiactividad. La guía *Security of Radioactive Sources*, además, transmite hechos y datos. Por ejemplo, en el apartado sobre la clasificación de las fuentes radiactivas, el Cuadro 3 indica los niveles de actividad de los diferentes radionucleidos de acuerdo con el umbral de categoría. Estos son datos técnicos que se presentan para dar sustento a las recomendaciones que ofrece la guía en materia de protección de fuentes radiactivas. Todos estos aspectos de contenido de la guía concuerdan con las características de un texto técnico.

Los temas que se mencionaron en el párrafo anterior y el contenido en general de esta guía también tienen un propósito. Al describir en la sección anterior el sistema de publicaciones del OIEA, se comprobó que este texto, al igual que toda la colección *IAEA Nuclear Security Series*,

tiene como objetivo general proteger las fuentes radiactivas y nucleares contra posibles usos dolosos. Sin embargo, el texto en estudio intenta cumplir un objetivo en particular. En su introducción se dedica un párrafo a explicar que esta publicación busca servir de guía para los Estados, las autoridades reguladoras y los operadores en la creación de reglamentos y programas de seguridad física de las fuentes radiactivas a lo interno de los Estados y de las organizaciones (1-2). El carácter práctico de estos objetivos en la protección del material radiactivo da soporte a la tesis de que esta guía es un texto técnico, a diferencia de un texto científico que buscaría la difusión de nuevos conocimientos dentro de un área especializada.

La manera de presentar la información también caracteriza al texto en estudio como técnico. La guía, en primer lugar, está redactada de forma impersonal. En ningún lugar del documento se hace mención a un individuo en particular, sino que se hace referencia al OIEA u otros organismos internacionales. Como parte de su enfoque, no busca sentar responsabilidades sobre personas específicas, sino dar recomendaciones que podrían ser aplicadas por los Estados, los organismos o las instituciones en la elaboración de reglamentos internos. En segundo lugar, la guía es concisa. En la sección dedicada a su alcance, es clara al indicar que se aborda únicamente la protección de las fuentes radiactivas, no así el transporte, el almacenamiento o las instalaciones donde se utilizan ni tampoco la protección del material nuclear (2). Además, en varios segmentos se menciona que la guía contiene los elementos mínimos que deberían incluir los reglamentos, por lo que excluye información innecesaria. El texto está dirigido a una audiencia en particular. En este caso, como se mencionó en el párrafo sobre sus objetivos y propósito, la guía está explícitamente dirigida a los Estados, las autoridades reguladoras y los operadores de fuentes radiactivas en la elaboración de sus reglamentos. Al hacerlo, sigue un estilo y formato particular. Puesto que la guía pertenece a una colección de publicaciones, es

posible notar que todos estos textos coinciden en la diagramación, la distribución de la información, la organización (numeración de las secciones) y las características tipográficas.

Como parte de la colección *IAEA Nuclear Security Series*, esta guía, una vez lista, queda a disposición del público en general para su consulta, incluso si llegara a quedar obsoleta por existir una versión más actualizada, lo cual revela su carácter de archivo. La guía también hace referencia a otros autores o textos. En este caso, al ser parte de una colección sobre seguridad nuclear y tener como base convenios y acuerdos internacionales, es común ver referencias a otros textos. Por esto, es posible que en otras publicaciones se haga referencia a la guía *Security of Radiactive Sources* y confirme su condición de archivo.

En conclusión, las características de los textos técnicos desarrolladas por Budisnki, las cuales se discutieron en el aparato crítico, se ven reflejadas en la guía en estudio. Dichas características afectarán las decisiones que se tomen en la traducción ya que el texto traducido deberá replicar las características del texto original. Además, las particularidades del texto dan pie a la identificación de necesidades informativas relacionadas con un campo técnico, las cuales se desarrollarán en las siguientes secciones de este capítulo.

2.4. Identificación de las necesidades informativas del texto original

Habiendo identificado el contexto documental dentro del cual se desarrolla la guía en estudio y el tipo de texto, el siguiente paso consiste en identificar las necesidades informativas con base en la propuesta de Merlo Vega y Arroyo Izquierdo en «Documentación y traducción: ámbitos de convergencia de dos disciplinas transversales». Como se explicó en la sección de metodología, la presente investigación gira en torno a tres tipos de necesidades informativas que un traductor debe solventar para verter el documento a otro idioma: las terminológicas, las

temáticas y las referenciales. A continuación se presentan las mismas junto con algunos ejemplos.

2.4.1. Necesidades informativas terminológicas

Al tratarse de un texto técnico, los traductores se enfrentarán a un léxico que no es el usual en los textos generales o las conversaciones informales. En cambio, surgirán términos especializados que será preciso identificar y entender dentro del contexto para, más adelante, poder encontrar su equivalente adecuado en español. Como se explicó en la sección anterior sobre las características del tipo de texto, la guía transmite datos técnicos y busca cumplir un objetivo: proteger las fuentes radiactivas. Por lo tanto, el texto traducido debe ser claro y preciso en la manera de presentar la información y en el uso de la terminología. Particularmente en el caso de la guía *Security of Radioactive Sources*, el traductor deberá asegurarse de que el mensaje sea trasmitido de manera que los usuarios finales puedan elaborar reglamentos que protejan las fuentes radiactivas, de acuerdo con las recomendaciones del OIEA. En esta sección se analizarán algunos ejemplos de necesidades informativas que surgieron a partir de la terminología empleada en el texto original. Las técnicas recomendadas para resolver esas necesidades mediante la documentación serán explicadas en el tercer capítulo de este trabajo.

2.4.1.1. *First responders*

El primer ejemplo es *first responders*. Este término no está definido en el texto original, a diferencia de otros que están incluidos en el glosario que se encuentra al final de la guía *Security of Radioactive Sources*. La primera vez que se menciona este concepto es cuando el texto hace referencia a los niveles de seguridad física, específicamente a la manera de responder ante actos dolosos. La siguiente oración cita la primera instancia en la cual se usa el término:

> The operator should develop procedures for reporting of security events to the regulatory body, **first responders**, and others as appropriate within a time frame required by the regulatory body commensurate with the security significance of the event. (34)

Además de esta cita, en una de las páginas anteriores, se había utilizado únicamente el término *responders* de la siguiente manera:

> Immediate means that **responders** should arrive, once notified, in a time shorter than the time required to breach the barriers and perform the tasks needed to remove the source. (31)

A partir de estos dos enunciados, sería posible inferir que los *first responders* son las personas o los organismos encargados de actuar ante una situación de emergencia, pero no establece exactamente cuáles. En primer lugar, era necesario averiguar si esa inferencia coincidía con la definición que maneja el OIEA. El hecho de que no estuviera definida en el texto original creaba un vacío de conocimiento que se debía llenar. En segundo lugar, una vez que se consiguiera la definición del término bajo el contexto de la seguridad física de fuentes radiactivas, era aún necesario buscar el equivalente más apropiado en español para el texto a traducir, proceso que se llevaría a cabo en la etapa onomasiológica del proceso de traducción y que quedará documentado en el Capítulo 3 de esta investigación.

2.4.1.2. *Security y safety*

El segundo ejemplo de necesidad terminológica es el caso de las palabras *security* y *safety* cuando son usadas de manera diferenciada en el texto original. Se puede asumir que ambos términos son conocidos por la mayoría los hablantes del inglés, incluidos los traductores, y hasta podrían considerarse sinónimos. Sin embargo, la guía *Security of Radioactive Sources* presenta oraciones como las siguientes:

a. The Code of Conduct recognizes that an effective national system of regulatory control underpins the **safety** and **security** of radioactive sources in a State (3).

b. **Safety** measures and **security** measures have in common the aim of protecting human life and health and the environment. **Safety** measures and **security** measures should be designed and implemented in an integrated manner so that **security** measures do not compromise **safety** and **safety** measures do not compromise **security** (10).

c. Within premises, interlock doors that meet **safety** requirements can serve the interests of **security** by controlling the movement of personnel and allowing staff to monitor access to the facility (51).

En casos como el del segmento a., el traductor podría saltar a la conclusión de que ambos términos se utilizan de manera indiferenciada; sin embargo, conforme avanza el texto, y como se puede observar en los segmentos b. y c., se empieza a notar una distinción entre ambos. Fruto de no precisar aún el alcance de cada término, nace otra necesidad informativa terminológica. Tener clara la distinción es fundamental porque la temática del texto, como indica incluso el mismo título del documento original, será únicamente la «security of radioactive sources». Una vez identificados ambos términos, será necesario encontrar sus equivalentes en español según el OIEA de manera que se traduzcan de forma precisa. Como se verá en el Capítulo 3, algunas técnicas de documentación pueden ayudar a abordar y solventar este tipo de problema traductológico.

2.4.1.3. *Design basis threat y DBT*

El tercer ejemplo que se analizará en relación con las necesidades informativas terminológicas es «design basis threat» y su sigla «DBT». Este término viene claramente explicado en el punto 3.8.2 del texto original y definido en su glosario. Se indica que es una

«comprehensive description of the motivations, intentions, and capabilities of potential adversaries against which protection systems are designed and evaluated» (65). La necesidad informativa traductológica surge a partir de la manera de traducirlo y abreviarlo en español. Según lo indicado en la guía *Security of Radioactive Sources,* los Estados o los organismos evalúan las diferentes amenazas contra las que habría que proteger las fuentes radiactivas. Con base en la información que se obtiene sobre estas amenazas es que se diseñan los sistemas de protección. Surgió entonces la duda de si este término se podría traducir como «la amenaza como base de diseño» o si se podría eliminar el artículo «la». Tampoco quedaba claro si se entendería que se hacía referencia al diseño de sistemas de seguridad física, o si era necesario explicitarlo en un término en español que fuera «la amenaza como base de diseño de los sistemas de seguridad física». Dada la extensión de esta última propuesta, otra opción que se podría contemplar fue una versión simplificada: «amenaza base de diseño». Sin embargo, se cuestionó el uso de un calco frente a una posible traducción libre que se ajuste a la normativa del español culto. Aunada a estas dudas, surgió también la necesidad de saber si era pertinente referirse a este término como sigla. En caso de que fuera apropiado, se analizó si mantener la sigla en inglés o utilizar un equivalente en español con base en la traducción del término. Había entonces que investigar mediante estrategias de documentación cuál era la opción más acertada para que el texto fuera no solo claro, sino consistente con la terminología de las otras publicaciones del OIEA.

2.4.2. Necesidades temáticas

Al lidiar con un texto técnico, el traductor también debería familiarizarse con el área de conocimiento a la cual pertenece el texto original. Es usual que debido a los plazos de entrega impuestos por el cliente, el traductor no pueda estudiar a fondo todos los temas que se

desarrollan en el contenido. Por esta razón, definir necesidades informativas temáticas desde un inicio podría ayudar a encontrar las fuentes documentales que realmente ayuden a resolver problemas relacionados con el contenido del texto. Conocer los temas que se discuten en el texto original permite conocer la terminología, la fraseología, el formato y la manera de presentar la información en el contexto dado. Para los objetivos de este trabajo, en este capítulo se analizarán algunos ejemplos de necesidades informativas temáticas que surgieron a partir del contenido del texto original.

2.4.2.1. Fuentes radiactivas

Un tema general sobre el cual se debería tener alguna noción es las fuentes radiactivas. Al leer esta guía, el traductor se podría plantear múltiples preguntas como las siguientes:

a. ¿Qué es una fuente radiactiva?
b. ¿Cómo se clasifican?
c. ¿Qué es la radiactividad?
d. ¿Cuáles son sus usos?
e. ¿En dónde se ubican las fuentes radiactivas?
f. ¿Quienes manejan las fuentes radiactivas?
g. ¿Existen fuentes radiactivas en Costa Rica?
h. ¿Dónde están ubicadas?

Cada una de estas preguntas podría acarrear diferentes inquietudes, particularmente con miras a la traducción del texto. Por ejemplo, mediante varios cuadros, la guía hace referencia a la clasificación de las fuentes radiactivas, a partir de la cual se generan diferentes niveles de seguridad física. Resultaba necesario, entonces, averiguar si el sistema de clasificación era universal o si sería necesario hacer aclaraciones para los usuarios finales de esta guía. Utilizar

las técnicas apropiadas de documentación garantizaría que el conocimiento adquirido fuera el pertinente y que no se utilizara tiempo de más en fuentes documentales que no fueran realmente útiles.

2.4.2.2. *Amenazas a la seguridad física de las fuentes radiactivas*

Otro tema que planteó problemas para la comprensión del texto y su respectiva traducción fueron las amenazas a la seguridad física. Si bien la guía *Security of Radioactive Sources* aborda la seguridad de las fuentes radiactivas, el traductor podría considerar necesario conocer más acerca de las amenazas, es decir, contra qué hay que protegerlas y por qué es necesario hacerlo. A primera vista pareciera un tema común, pero deja de serlo cuando existen organismos internacionales dedicados a explicarles a los Estados, las autoridades reguladoras y los operadores cómo proteger las fuentes radiactivas y cómo crear marcos regulatorios para ejecutar dicha protección. Es más, uno de los puntos de la guía versa sobre la manera de entender y abordar las amenazas, incluida la definición de la amenaza a nivel nacional, cómo responder ante una amenaza específica, la identificación de amenazas dentro de las organizaciones o instituciones, entre otros temas relacionados; sin embargo, al ser una guía general, no se especifican cuáles podrían ser esas amenazas. Al traductor le serviría además entender por qué era necesario una cultura de la seguridad física y sus distintos componentes para defenderse de las amenazas. Contra qué o quién están siendo protegidas las fuentes es un aspecto fundamental para entender los contenidos desarrollados en el texto original. Distinguir cuáles fuentes documentales son las más útiles para llenar este vacío de conocimiento es uno de los objetivos de contar con un método adecuado de documentación.

2.4.2.3. *Should*

El modal *should* se repite en muchos de los enunciados de la guía *Security of Radioactive Sources*. Un ejemplo de su uso es el siguiente:

Care **should** be taken to ensure that intrusion detection measures cannot be bypassed (27).

Varias obras consultadas para este estudio afirmaban que se da por sentado que el traductor tiene un conocimiento avanzado de los idiomas con los que trabaja. *Should* no es un término técnico y más bien pertenece al vocabulario básico de una persona hablante del inglés. Dependiendo del contexto, este modal se tiende a asociar a palabras en español como «debe», «debía» o «debería». El primer impulso podría ser traducirlo como uno de esos equivalentes. Es más, en los borradores de la traducción del texto en estudio, en algún momento se utilizó «debe» y «debería» de manera intercambiable. Sin embargo, en la introducción de la guía se indica que esta tiene la función de servir como orientación para el proceso la elaboración de los reglamentos en materia de seguridad física, lo que significa que lo que ahí se indique no tiene carácter vinculante para ningún organismo o Estado. Este último razonamiento fue el que llevó a pensar que *should* respondía más a una necesidad temática que a una terminológica, aunque se podría argumentar que está en el límite entre las dos pues se trata de una unidad léxica. No obstante, dado el contenido de la guía, esta opción se tuvo que valorar de nuevo. Por medio de técnicas de documentación se buscó la forma de resolver esta incógnita y traducir *should* de modo que conservara el mismo peso semántico que el de la guía *Security of Radioactive Sources*; la respuesta a esta interrogante se analiza a profundidad en el tercer capítulo de esta investigación.

2.4.3. Necesidades referenciales

En la sección donde se describen las características de los textos técnicos, se indicó que la guía *Security of Radioactive Sources* cumplía con la particularidad de hacer referencia a otros

textos del OIEA. No obstante, al leer el documento se descubrió que la manera de hacerlo respondía a un estilo muy propio del sistema de documentación de dicho organismo. Cuando se cita o se remite a otros documentos, la guía lo hace de las siguientes maneras:

a. Se indica el nombre del documento seguido del número de referencia entre corchetes. Por ejemplo, «It will also assist State parties to fulfil certain obligations under the **International Convention for the Suppression of Acts of Nuclear Terrorism [7]**» (1).

b. Se omite el nombre y solo se utiliza la partícula «Ref. [número de referencia]». Por ejemplo, «Such guidance, including that for third party shippers, is given in **Ref. [12]**» (2).

c. Se omite el nombre y la partícula «Ref.»; solo se indica el número de referencia entre corchetes. Por ejemplo, «Such guidance is available in other IAEA publications **[5, 9, 10]**» (2).

Los números que aparecen después de cada una de las referencias ayudan a organizar la bibliografía al final del documento y facilitan la ubicación de las entradas en dicha parte de la guía. Las diferentes formas de presentar las referencias en el texto hicieron surgir la duda de si sería pertinente estandarizar el estilo en la traducción para favorecer la claridad del texto o si sería mejor mantener el estilo del texto original. Además, la manera en la que se aborden las referencias dentro del texto podría afectar las decisiones que se tomaran para la sección de «Referencias» al final de la guía y, a su vez, verse afectada por ellas, tema que se comentará a continuación.

Como se mencionó en el párrafo anterior, la sección «Referencias» por sí misma representa otro reto traductológico. Las entradas de cada fuente incluyen los siguientes datos separados por comas, en el orden en que se despliega a continuación:

a. El autor en mayúsculas,

b. El nombre del documento,

c. La colección a la cual pertenece la referencia y el número de publicación,

d. Editorial,

e. El lugar y el año de publicación, este último entre paréntesis.

A partir de esos datos, el traductor podría hacerse las siguientes preguntas:

a. ¿Debería mantener los nombres de los documentos en inglés, traducirlos o solo traducirlos si se encuentra una versión oficial en español?

b. En el caso de los organismos o instituciones, ¿debería mantener los nombres en inglés, traducirlos o solo traducirlos si se encuentra una versión oficial en español?

c. ¿Debería mantener la separación de los datos mediante comas o estandarizar su redacción a un formato de referencias reconocido como APA, *Chicago Manual of Style* o CBE?

Además de estas preguntas, varias referencias bibliográficas suponían problemas traductológicos que requerían atención. En los siguientes párrafos se comentan algunos ejemplos y en el tercer capítulo se ilustrarán las estrategias de documentación que ayudarán a resolver tales problemas.

A lo largo de la guía *Security of Radioactive Sources*, se remite continuamente a segmentos del *Code of Conduct on the Safety and Security of Radioactive Sources*. En el prefacio se indica que este documento fue creado en el 2003 como parte del interés creciente de los Estados en la protección de las fuentes radiactivas. Una búsqueda simple mediante el motor de búsqueda de Google permitió encontrar la versión oficial de este texto completo, el cual reúne, en un solo archivo, las versiones en inglés, árabe, francés, ruso, español y chino. En el caso de esta referencia, el reto surge al notar que la traducción de los términos *safety* y *security* en el título (seguridad tecnológica y seguridad física) de una obra de diez años de antigüedad podría no concordar con los resultados del proceso de documentación. Si como respuesta a la

necesidad informativa terminológica se tomaba una decisión diferente para la traducción de *safety* o *security*, persistía la duda de cómo referir entonces a este documento. Por un lado, si se empleaba en la referencia la versión del traductor, existía el riesgo de que se tornara confuso citar un documento con un nombre no oficial. Por otro lado, al citar el nombre oficial, la confusión podría surgir por la falta de congruencia en la terminología. Se comprobó que contar con la versión oficial traducida no era suficiente y que era necesario utilizar estrategias de documentación para encontrar la solución.

Otro ejemplo de necesidad informativa referencial surge cuando la guía hace referencia al documento llamado *Development, Use and Maintenance of the Design Basis Threat*. El glosario incluido en la guía *Security of Radioactive Sources* cuenta con una definición que fue adaptada a partir del documento en cuestión. En este caso, se define *design basis threat* de la siguiente manera:

> «A comprehensive description of the motivations, intentions, and capabilities of potential adversaries against which protection systems are designed and evaluated (adapted from Ref. [13])». (65)

En el resto del texto, se remite al lector a dicho documento, en el cual podrá encontrar más información sobre algunos temas. La siguiente cita es otro ejemplo:

> «More detailed information on the DBT process can be found in Ref. [13]». (12)

En este caso, el título de esta referencia no aparece explícitamente en el contenido del texto. A diferencia del *Code of Conduct on the Safety and Security of Radioactive Sources*, se consideró que esto eliminaba en parte la posibilidad de incongruencia de terminología dentro del texto. Sin embargo, el problema nació a raíz de la falta de una versión oficial en español a la que se pudiera remitir puesto que el título del documento sí aparece en la lista de referencias

al final del documento. Se mantenía, entonces, la interrogante de cómo proceder con estos títulos en inglés. Una opción era no traducirlos para que al lector le fuera factible utilizar el nombre del documento original en un motor de búsqueda y ubicarlo en caso de ser necesario. Esta opción acarreaba el riesgo de que el lector sin conocimientos del inglés no contara con la posibilidad de entender sobre qué se trataba el tema del texto referencia. Una segunda opción era traducir el nombre mediante técnicas de documentación para traducir el título. En este caso, el problema surgiría porque, al realizar una búsqueda en internet de un nombre no oficial, era posible que el lector no encontrara la fuente en caso de que la requiriera. Finalmente, se consideró una tercera opción, la cual consistiría en indicar el nombre en inglés y la propuesta de traducción entre corchetes. Aquí el problema sería la posibilidad de no ser consistente con los otros textos de la IAEA Nuclear Security Series en cuanto a la manera de presentar las referencias dentro del texto.

El caso del *IAEA Fundamental Safety Principles* también se convirtió en un reto. Es pertinente mencionar que, en el contenido de la guía, se hace referencia a esta publicación una sola vez, cuando se indica que forma parte de los textos con los cuales se debe leer la guía *Security of Radioactive Sources*. Aparte de la introducción, solo vuelve a aparecer en la sección de «Referencias», al final de la guía. No obstante, en ambas ocasiones aparece nombrada de manera distinta. En la introducción, aparece como «IAEA Fundamental Safety Principles» y, en las referencias, su título es «Fundamental Safety Principles IAEA Safety Standards Series». Ante esta diferencia, surgieron en primera instancia las dudas sobre cómo nombrarlo dentro del contenido del texto traducido, cuál era el nombre oficial y cómo proceder con su versión en español.

Tal como sucedió con el caso del *Código de Conducta*s, se comprobó que encontrar una versión oficial en español no siempre brindaba soluciones a los problemas traductológicos. Tal es el caso del documento titulado *International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, Safety Series No. 115*, el cual trajo otro reto, esta vez relacionado con la autoría. En la sección de «Referencias» de la guía en estudio, se listan como autores de esta publicación a las siguientes organizaciones e instituciones: European Atomic Energy Community, Food and Agriculture Organization of the United Nations, International Atomic Energy Agency, International Labour Organization, International Maritime Organization, OECD Nuclear Energy Agency, Panamerican Health Organization, United Nations Environment Programme y la World Health Organization. Sin embargo, en el texto oficial traducido (que se titula *Normas básicas internacionales de seguridad para la protección contra la radiación ionizante y para la seguridad de las fuentes de radiación, Colección Seguridad No 115*), todas ellas aparecían como patrocinadoras, mas no como autoras. Esto representaba un nuevo reto sobre la manera en la que se presentarían dichos organismos en las páginas de referencia. Además, en caso de que estas organizaciones se incluyeran como autoras, habría que buscar el nombre oficial de cada una de ellas en español. En caso de que no existiera ese nombre en la lengua meta, vendría el reto de cómo abordar la presentación de las mismas en el texto traducido. Para determinar la forma correcta de proceder, era necesario acudir a estrategias adecuadas de documentación, tarea que será abordada en el siguiente capítulo.

2.5. Conclusión

Las necesidades identificadas en esta fase semasiológica sientan las bases para las soluciones que se deberán emplear en la etapa onomasiológica. Como parte de las estrategias de

documentación que se proponen en este trabajo, se pretende que la identificación de dichas necesidades ahorre tiempo al traductor, pues sabrá específicamente qué buscar y dónde buscarlo. Además, como se verá en el próximo capítulo, las soluciones documentales que serán exploradas en la siguiente etapa en ocasiones brindan respuesta a más de una necesidad, pues la idea es utilizar técnicas que lleven a contar con un sistema ordenado y sistematizado que evite perder de vista los recursos que ya se hayan encontrado y que podrían ser útiles en encargos de traducción futuros. Las necesidades informativas, temáticas y referenciales que se identificaron en la guía *Security of Radioactive Sources* se consideran similares a las que podrían aparecer en otras publicaciones de la IAEA Nuclear Security Series, por lo que futuros traductores de estas y otras publicaciones relacionadas podrían identificarse con los problemas traductológicos aquí planteados.

Capítulo 3 – Etapa onomasiológica para la traducción de la guía *Security of Radioactive Sources*: Búsqueda y evaluación de recursos documentales electrónicos

3.1. Introducción

En este capítulo se aborda la segunda parte del método de documentación propuesto para la traducción de la guía *Security of Radioactive Sources*, en este caso, en su fase semasiológica. El propósito de este apartado es describir el proceso de recolección, análisis y evaluación de fuentes que puedan ayudar a resolver las necesidades informativas de la guía en estudio. Para la fase de recolección, se seguirán las recomendaciones de Merlo Vega en relación con el orden de las búsquedas de recursos documentales. Como se mencionó en el aparato crítico, en este capítulo se utilizarán las búsquedas sobre terminología especializada, de información sobre la materia y de textos paralelos; estas búsquedas encabezarán cada una de las tres secciones de este apartado. Para ejemplificar el proceso de recolección de fuentes, se utilizarán algunas de las necesidades terminológicas, temáticas y referenciales planteadas en el Capítulo 2. Al inicio de las búsquedas sobre terminología especializada y de información sobre la materia, se explicarán los parámetros de búsqueda; en el caso de los textos paralelos, se explicará el proceso de selección de fuentes a ser analizadas. Después, se analizarán algunos documentos y se evaluará su utilidad para la traducción que se está realizando. Como parte de las estrategias de documentación propuestas, se crearon además fichas descriptivas como registro de las fuentes consultadas. Estas fichas se encuentran en los anexos 1-18. Los parámetros y criterios incluidos en las fichas se tomarán como base para la evaluación de los recursos documentales. Cabe destacar que se consideró que todas las fuentes incluidas en este análisis cumplen con los criterios de gramática y vocabulario, por lo que no fueron analizados en las evaluaciones.

3.2. Búsqueda de recursos sobre terminología especializada

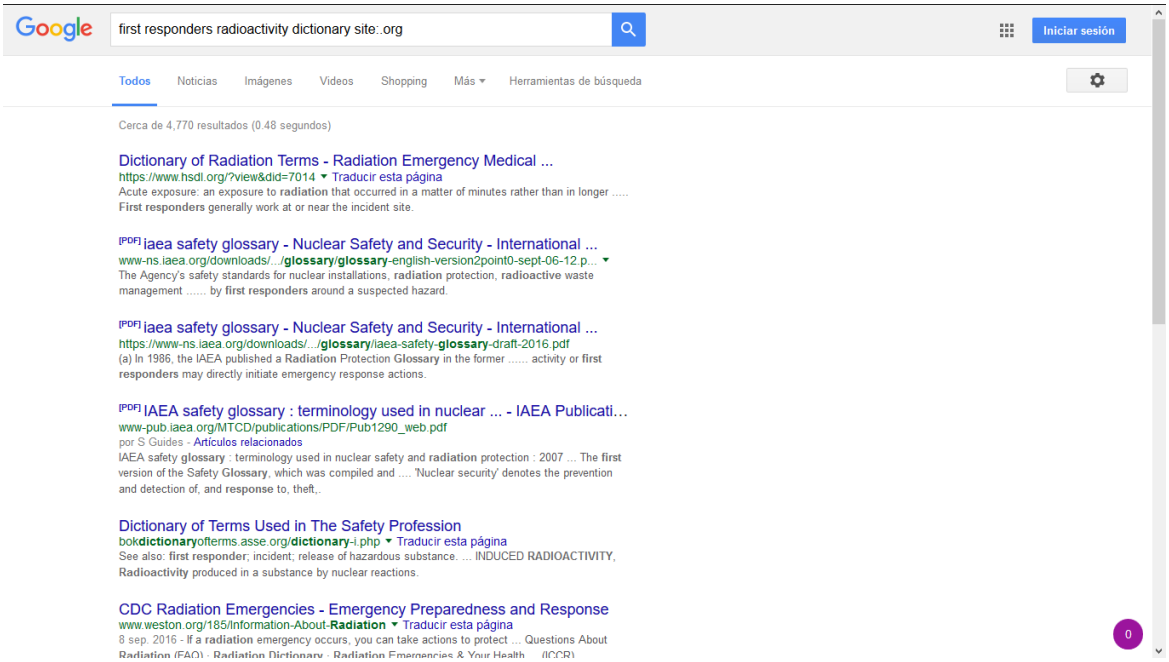
Esta sección del capítulo está dividida en dos secciones, una dedicada a recursos monolingües y otra dedicada a recursos bilingües, los cuales serían los recursos básicos que utilizaría un traductor. Para ilustrar el proceso de búsqueda, se utilizarán los términos mencionados en la sección de «Necesidades informativas terminológicas» del Capítulo 2, con el propósito de evaluar la capacidad de algunas de las fuentes documentales encontradas para resolver los distintos problemas terminológicos. Para recopilar las fuentes se utilizó la función avanzada del motor de búsqueda de Google. Con el propósito de recrear los pasos que podría tomar un traductor, en cada caso se ingresaron términos de búsqueda junto con diferentes frases que ayudaran a obtener los recursos necesarios. Durante el proceso de investigación, se utilizaron diferentes frases para acompañar el término para el cual se buscaba definición o equivalente en español, pero esta estrategia daba como resultado documentos relacionados con las fuentes radiactivas, no glosarios ni diccionarios especializados. Para poder encontrar recursos sobre terminología especializada, era necesario descartar varios resultados y pasar varias páginas. Con las frases elegidas, las cuales serán indicadas en cada ejemplo de búsqueda analizado, se logró obtener de manera más expedita glosarios o diccionarios especializados. Por otra parte, la búsqueda se configuró de manera que el sitio o dominio perteneciera a alguna organización u organismo que pudiera ofrecer recursos o fuentes oficiales; para ello, en los términos de la búsqueda se utilizó el operador «site:.org», el cual da como resultados sitios cuyo dominio sea .org (organismos y organizaciones sin fines de lucro). Al estar lidiando con un texto elaborado por un organismo internacional, se consideró necesario obtener fuentes documentales que tuvieran un respaldo estatal o institucional. No se utilizó la búsqueda de una frase exacta porque se buscaban definiciones en lugar de un uso en contexto. Para que el lector pueda visualizar esta parte del proceso, se incluye una captura de pantalla con los resultados de la

búsqueda y se analizan dos de estos resultados. Finalmente, para evaluar cada recurso documental, se utilizarán los parámetros incluidos en una ficha documental por recurso.

3.2.1. Búsqueda de diccionarios o glosarios especializados monolingües

Como se comentó en el capítulo anterior, se consideró necesario encontrar la definición de algunos términos para tener claro su significado antes de buscar su traducción. Para recrear el proceso de traducción y obtener diccionarios o glosarios especializados monolingües, en esta etapa se buscaron términos en inglés con su respectiva definición en el mismo idioma mediante el buscador Google. Uno de los ejemplos de necesidades terminológicas que se planteó en el segundo capítulo fue *first responders*. Los términos de búsqueda elegidos para este ejemplo fueron «first responders radioactivity dictionary site:.org», con los cuales se obtuvieron los resultados que se ilustran en la siguiente imagen:

Imagen 3. Búsqueda de diccionarios o glosarios especializados monolingües



En los siguientes párrafos se evalúan los primeros dos resultados con base en su utilidad para resolver necesidades informativas terminológicas.

3.2.1.1. «Dictionary of Radiation Terms»

El primer resultado que se obtuvo fue el «Dictionary of Radiation Terms», para el cual se creó una ficha descriptiva que se puede encontrar en el anexo 2. En esta fuente, se define *first responders* como las primeras personas encargadas de responder a una emergencia, las cuales suelen ubicarse en lugares cercanos al lugar del incidente. Esto coincide con lo que se había inferido a partir del contexto de la guía en análisis. Por otra parte, no fue posible ubicar los otros términos planteados en el segundo capítulo de este estudio (*safety*, *security* y *design basis threat*). Debido al alcance de esta investigación, no se buscaron otros términos que representaran un problema traductológico, pero se reconoce que podrían estar en este diccionario dadas las características que se mencionarán en los siguientes párrafos.

Descripción general y autoría

El «Dictionary of Radiation Terms» aclara que se trata de una versión creada por la Radiation Emergency Medical Management (REMM, por sus siglas en inglés) a partir del «Radiation Dictionary», elaborado por Centers for Disease Control and Prevention. En la página «About this site», se indica lo siguiente en relación con el origen de la REMM:

> REMM was produced by the Department of Health and Human Services, Office of the Assistant Secretary for Preparedness and Response, Office of Planning and Emergency Operations, in cooperation with the National Library of Medicine, Division of Specialized Information Services, with subject matter experts from the National Cancer Institute, the Centers for Disease Control and Prevention, and many US and international consultants.

Además de los agentes involucrados en la creación de los contenidos, se listan siete personas como encargadas del sitio web, dos de las cuales son radioterapeutas, dos asesores médicos y una especialista en sistemas de información (REMM). La mayoría de los expertos mencionados destacan por estar especializados en áreas de conocimiento relacionadas con el uso de la radiación. Esta información brinda credibilidad a los contenidos que se puedan encontrar en el diccionario.

En cuanto al contenido, esta fuente ofrece un listado de términos técnicos relacionados con la radiación y su uso en la medicina. Las entradas están en orden alfabético y cuentan con su respectiva definición en inglés. Se considera que las definiciones están dirigidas a un segmento de la población acostumbrado a la jerga médica relacionada con el uso de la radiación. Además, dentro de cada definición, algunas palabras son enlaces que llevan a otras páginas, en las cuales se ilustra más claramente un término, se da una explicación más exhaustiva o se salta a otro segmento del diccionario donde se define el término en particular. Otro aspecto muy útil del diccionario es que al inicio se ofrece un listado de enlaces a diferentes glosarios relacionados con el tema, algunos de los cuales pertenecen al OIEA. Al momento de realizar este estudio, en setiembre del 2016, se indicaba que la fecha de actualización del diccionario databa del 16 de agosto del 2016, lo cual denota su fiabilidad como fuente documental revisada y vigente. En cuanto al contenido, el único aspecto que se podría considerar negativo es que la REMM no tiene relación con el OIEA, por lo que en búsquedas posteriores se podría intentar ubicar un diccionario o glosario afiliado a tal organismo. Aun así, como primer resultado de búsqueda, se considera que este diccionario podría ser de gran valor no solo como fuente para encontrar definiciones, sino como punto de partida para ubicar otros glosarios o textos que pudieran ser útiles en la resolución de otras necesidades informativas.

Compatibilidad, funcionabilidad, navegabilidad y diseño

El diccionario está en formato HTML, lo cual hace que sea fácil desplazarse a las diferentes secciones o enlaces de la página, especialmente mediante comandos de teclado. No obstante esta navegabilidad dificulta la impresión del documento en un formato que sea completamente amigable con el usuario y depende de una conexión a internet. Si bien es posible ubicar herramientas de software que resuelvan esta dificultad, la fuente documental por sí sola no la ofrece. A pesar de que la estructura y la organización son adecuadas, el diccionario se presenta en una sola página web sin divisiones, lo que afecta el formato de impresión como se acaba de mencionar. Otro punto negativo es que no cuenta con un menú siempre visible que facilite pasar a diferentes secciones. Al inicio, se ofrecen accesos directos a las letras que componen los términos del diccionario, pero una vez que se llega a una letra en particular, es necesario devolverse manualmente al inicio para buscar y seleccionar otra letra. A pesar de la falta de un menú funcional, se consideró que otros aspectos del diseño, como los colores y la tipografía, sí son adecuados.

Pertinencia y conclusiones

Se considera que si bien el «Dictionary of Radiation Terms» de la REMM no cumplió con todos los aspectos de formato, el contenido es de mucho valor y no se debe obviar su credibilidad como fuente documental para resolver problemas de carácter terminológico en la traducción de la guía *Security of Radioactive Sources*. Dada la particularidad del OIEA como una organización con un gran número de publicaciones oficiales, incluidos glosarios (como se verá más adelante), el valor del «Dictionary of Radiation Terms» queda relegado por no tener una conexión directa con dicho organismo y el contenido de la guía que se está traduciendo. Como fuente documental, su contenido solo podría cubrir necesidades informativas terminológicas. Si bien ofrece enlaces

a páginas externas que puedan cubrir necesidades temáticas, ellas requerirían un análisis profundo y aparte. Por tanto, como primer resultado de búsqueda, es una fuente documental de calidad, pero que posiblemente se relegaría a segundo plano si se encuentran publicaciones del propio OIEA.

3.2.1.2. *IAEA Safety Glossary*

El segundo resultado fue el *IAEA Safety Glossary*, cuya ficha descriptiva se puede consultar en el anexo 3. En este glosario, *first responders* se define como «The first members of an emergency service to respond at the scene of an emergency» (58). En esta definición, *emergency service* remite a otra parte del glosario donde se indica que son organismos externos, como «police, fire fighters and rescue brigades, ambulance services and control teams for hazardous materials» (48) los encargados de atender las emergencias. Esta definición brinda información más detallada en comparación con la que se había inferido a partir del contexto y la definición ofrecida por el diccionario de la REMM. Como se indicó en el capítulo anterior, *design basis threat* estaba definido dentro de la guía *Security of Radioactive Sources*; aun así, a modo de ejercicio, se buscó en este glosario, pero no se encontró. Sin embargo, *design basis* sí aparece y está definido como «the range of conditions and events taken explicitly into account in the design of a facility» (51). Esta definición, a manera de complemento de lo indicado en la guía, podría ayudar a comprender de mejor manera el concepto de *design basis threat* .

Por otra parte, este glosario ayudó a resolver otros problemas traductológicos. Aparece el término *safety*, el cual remite al término *nuclear safety*, cuya definición indica que se refiere a «the achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in the protection of workers, the public and the environment from undue radiation hazards» (102). Mientras tanto, *security* remite a *nuclear security*, la cual

se define como «prevention and detection of and response to, theft, sabotage, unauthorized access, ilegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities» (102). En primer lugar, esta segunda definición coincide con lo que se desarrolla en la guía *Security of Radioactive Sources* y la Nuclear Security Series en general. En segundo lugar, aclara la duda planteada en el segundo capítulo sobre la manera de diferenciar el significado de los términos *safety* y *security*. A partir de haber encontrado estas dos definiciones, empieza a quedar claro que *safety* se refiere a la protección de personas y medio ambiente ante accidentes radiológicos, mientras que *security* se refiere a la protección de las fuentes radiactivas para evitar que sean utilizadas en actos dolosos. Como resultado, se podría decir que este glosario, además de resolver una necesidad informativa terminológica, también podría estar resolviendo una necesidad informativa temática al aclarar el verdadero alcance de la guía que se está traduciendo. En los próximos párrafos se analizará la fiabilidad de este recurso documental.

Descripción general, autoría y contenido

Uno de los aspectos que más destaca es el OIEA como autor de esta publicación, el cual también lo es de la guía que se está traduciendo. En cuanto a los contenidos, es un glosario monolingüe de seguridad radiológica. Los términos están en orden alfabético, incluyen su respectiva definición y, de ser necesario, añaden aclaraciones. Además, otra característica importante es que dentro de las definiciones suelen aparecer palabras en cursiva, con lo cual se indica que pueden encontrarse definiciones de las mismas en otras partes del glosario en caso de ser necesaria su aclaración; por ejemplo, en párrafos anteriores se mencionó el caso de *emergency services* dentro de la definición de *first responders*. Esta publicación data del 2007, lo que se considera relativamente reciente al momento de realizar esta investigación, en

setiembre del 2016, y por lo tanto útil para su uso en la traducción de la guía *Security of Radioactive Sources*, publicada en el 2009. Contar con un glosario creado por el mismo organismo que elaboró el texto que se está traduciendo brinda bastante fiabilidad a los contenidos que se encuentren pues, como se indica en sus primeras páginas, su propósito es armonizar el uso de la terminología a lo interno del OIEA (s. pag.). Además de todo lo mencionado, gracias a una de las búsquedas posteriores (que se comentará en la sección dedicada a diccionarios y glosarios bilingües), se encontró que cuenta con versiones en árabe, chino, francés, ruso y español, lo cual brinda nuevos recursos para resolver necesidades informativas terminológicas en la lengua meta.

Compatibilidad, funcionabilidad, navegabilidad y diseño

En cuanto a la manera de presentar la información, este glosario está publicado en formato PDF, por lo que en caso de que se necesite imprimir, mantendría el mismo formato que aparece en la pantalla. Además, también permite buscar palabras específicas mediante comandos como «Control+F». La información se muestra de manera lógica, pues al inicio se presenta una amplia introducción que incluye, entre otros aspectos, el alcance del glosario y una explicación de la manera de utilizarlo. El documento cuenta con un menú de marcadores funcional que permite desplazarse a los distintos segmentos del glosario de manera más fácil. Se considera que el diseño en general, los colores empleados y la tipografía utilizada fueron funcionales para un glosario formal y oficial de un organismo internacional.

Pertinencia y conclusiones

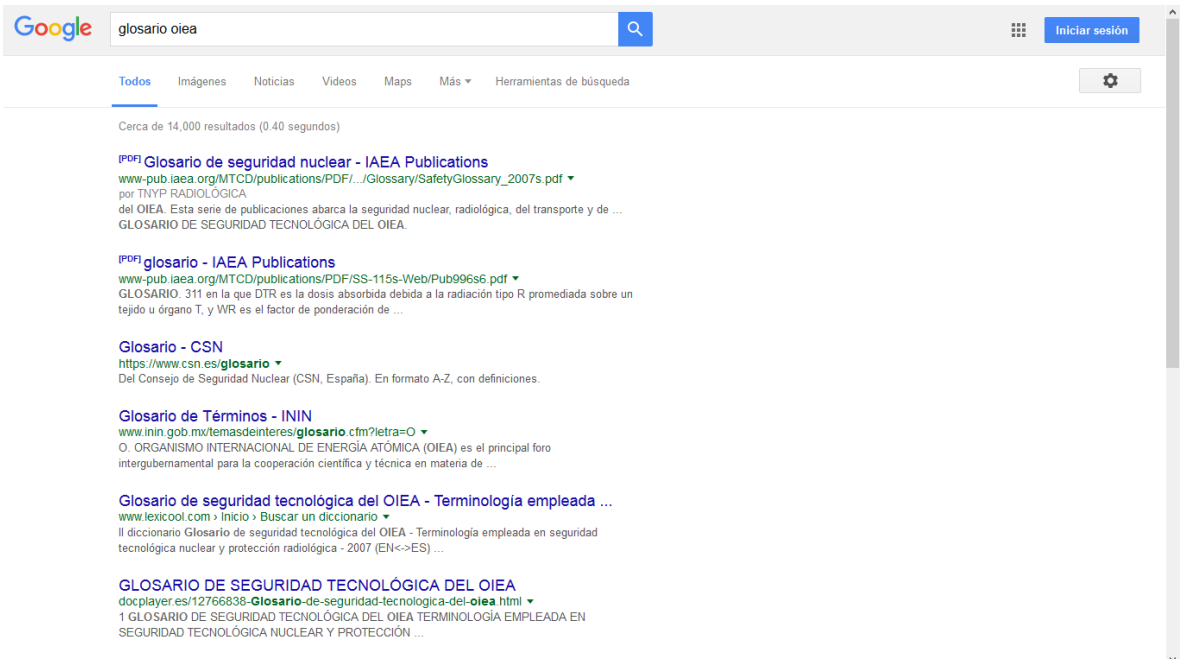
En conclusión, este glosario es de mucha utilidad para la traducción que se está realizando. Un aspecto fundamental es que fue posible encontrar definiciones claras de términos con los que se está trabajando en la guía *Security of Radioactive Sources*. Al haber sido creado por el

mismo OIEA y en un año reciente, los contenidos son fiables para el traductor, quien, como se comentó en párrafos anteriores, podría aclarar dudas de índole no solo terminológica, sino también temática al encontrarse las definiciones de, por ejemplo, *safety* y *security*. Los parámetros de diseño, navegabilidad y formato se consideraron funcionales para el traductor. Por lo tanto, se considera que el *IAEA Safety Glossary* es una fuente documental de mucho valor y fiabilidad para su uso en la traducción de diferentes publicaciones del OIEA, incluida la guía *Security of Radioactive Sources*.

3.2.2. Búsqueda de diccionarios o glosarios bilingües

Como traductores, los diccionarios y glosarios bilingües son sumamente útiles para encontrar términos equivalentes en otros idiomas. En el segundo capítulo de este trabajo, se comentaron ejemplos de términos para los cuales ya se contaba con una definición en inglés, pero para los que su equivalente en español se mantenía como una necesidad informativa terminológica. Como parte del ejercicio de traducción, se planeó utilizar una metodología similar a la búsqueda en Google de diccionarios o glosarios especializados monolingües, es decir, mediante el uso de un término en particular junto con palabras que ayudaran a obtener diccionarios o glosarios bilingües. Sin embargo, este método no arrojó los resultados esperados para ejemplificar esta fase de búsquedas porque el motor de búsqueda no devolvía diccionarios o glosarios como resultados de las búsquedas y, en caso de que lo hiciera, eran monolingües. Se intentó con diferentes palabras clave hasta que se llegó a la conclusión de que la mejor manera de obtener resultados bilingües era mediante las palabras sueltas «glosario oiea». En la siguiente imagen se ilustran los resultados:

Imagen 4. Búsqueda de diccionarios o glosarios bilingües



En los siguientes párrafos se evalúan los primeros dos resultados con base en su utilidad para resolver necesidades informativas terminológicas.

3.2.2.1. *Glosario de seguridad tecnológica del OIEA*

El primer resultado que se obtuvo fue el *Glosario de seguridad tecnológica del OIEA*, cuya ficha descriptiva se puede encontrar en el anexo 4. En este glosario, se encontraron los siguientes equivalentes para los ejemplos de necesidades informativas terminológicas mencionados en el Capítulo 2:

i. «Primeros actuantes» aparece como el término equivalente para *first responders* (148).

ii. «Seguridad física» aparece como el término equivalente para security (167).

iii. «Seguridad tecnológica» aparece como el término equivalente para *safety* (168).

iv. *Design basis threat* no aparece. Al igual que en la versión monolingüe en inglés, lo que se incluye es únicamente «base de diseño» como el término equivalente para *design basis* (21).

Como se puede notar, este glosario oficial contiene la mayoría de los términos que habían sido planteados como retos traductológicos en el segundo capítulo. En los siguientes párrafos se evaluará la fiabilidad de este recurso con base en los parámetros incluidos en las fichas descriptivas.

Descripción general, autoría y contenido

Este glosario fue publicado por el OIEA. El proceso de documentación que se ha realizado hasta el momento hace que, en este punto de la investigación, se conozcan las ventajas de contar con un glosario creado por el mismo organismo creador de la guía *Security of Radioactive Sources*. La forma de presentar los términos coincide en su mayoría con la versión en inglés de este glosario, el *IAEA Safety Glossary*. Los términos en español se presentan en orden alfabético junto con su respectiva definición en español y aclaraciones, de ser necesario. También se hace uso de cursivas para remitir a otros términos dentro de la misma publicación. Una diferencia con respecto a la versión monolingüe es que se indica el equivalente en inglés debajo de cada término en español. Otra característica relevante es que, al final del glosario, se incluye una sección en la cual se listan los términos en inglés en orden alfabético. Esto es útil para quienes traducen al inglés ya que, en la mayoría de los casos, los traductores desconocerían el término en español (razón principal por la que harían uso de este glosario). Una vez que se identifica el equivalente en la lengua meta, de ser necesario, se podría buscar su definición en español. Dada la distribución de los términos, se intuye que este glosario es para ser utilizado por hablantes del español que buscan definiciones de términos en su idioma; se podría pensar que el equivalente en inglés les sería útil, pero no indispensable. El *Glosario de seguridad tecnológica del OIEA* también fue publicado en el 2007, lo cual hace que sea fiable para su uso como fuente documental en la para la traducción de la guía *Security of Radioactive Sources*, del 2009.

Compatibilidad, funcionabilidad, navegabilidad y diseño

Este glosario está en formato PDF, por lo que en caso de imprimirse, el texto se mostraría de la misma manera que aparece en la pantalla, algo útil para el usuario, en este caso, el traductor. Además, mediante comandos como «Control+F» se pueden buscar palabras específicas, como los términos en inglés, y así dar con su equivalente en español. La información se muestra de manera lógica. Como su versión en inglés, al inicio del glosario se presenta una introducción donde se explica el alcance del glosario y su uso. Esta publicación también cuenta con un menú de marcadores que ayuda a movilizarse fácilmente a los distintos segmentos del glosario. En general, el diseño, los colores empleados y la tipografía utilizada se consideraron funcionales y adecuados para un glosario formal y oficial de un organismo como el OIEA.

Pertinencia y conclusiones

Como conclusión, este glosario genera bastante credibilidad para su uso en la traducción de la guía *Security of Radioactive Sources*. Un aspecto fundamental es que fue posible encontrar equivalentes oficiales de los términos sobre los que se tenían dudas. Además, al haber sido creado por el mismo OIEA en un año reciente, los contenidos son fiables para el traductor. Los parámetros de diseño, navegabilidad y formato se consideraron también funcionales para el traductor. Aparte de solventar necesidades informativas terminológicas, también resuelve necesidades referenciales, pues esta es una de las publicaciones citadas en la guía *Security of Radioactive Sources*. Gracias a este hallazgo, se cuenta con el título oficial en español de este glosario para incluirlo en la sección de «Referencias» de la guía en estudio. Por lo tanto, se considera que el *Glosario de seguridad tecnológica del OIEA* es una fuente documental de mucho valor y fiabilidad para su uso en la traducción de diferentes publicaciones del OIEA, incluida la guía *Security of Radioactive Sources*.

Como información adicional, cabe agregar que, tal como se comentó en su análisis, la mayoría de las características de este glosario coinciden con las de la versión homóloga en inglés, el *IAEA Safety Glossary*. Haber descubierto esta versión en español llevó a intentar, a modo de ejercicio, una búsqueda en Google del título en inglés de la obra. El primer resultado de dicha búsqueda consiste en una página del OIEA llamada «IAEA Safety Glossary», en la cual se ofrecen versiones de este glosario en árabe, chino, francés, ruso y español, datos que se agregaron a las fichas descriptivas. Esta búsqueda además hizo posible descubrir que, al momento de este hallazgo (setiembre del 2016), se ofrecía una nueva versión en inglés, con fecha del 2016. La misma se encontraba en período de revisión, fase por la cual deben pasar todas las publicaciones del OIEA, como se detalló en el segundo capítulo de este estudio. Con el objetivo de no desviarse de la metodología propuesta para esta investigación, se omitirán los comentarios relacionados con este glosario más reciente, el cual en su primera página indica que no se debe considerar como una versión oficial. Sin embargo, es preciso señalar que la aplicación de las estrategias de búsquedas pueden fortalecer el proceso de documentación que podría llevar a cabo un traductor, como lo demuestran estos resultados.

3.2.2.2. *Glosario de las Normas básicas internacionales de seguridad para la protección contra la radiación ionizante y para la seguridad de las fuentes de radiación*

El segundo resultado que se obtuvo fue el glosario de las *Normas básicas internacionales de seguridad para la protección contra la radiación ionizante y para la seguridad de las fuentes de radiación* (en adelante *Normas básicas internacionales*), cuya ficha descriptiva se puede encontrar en el anexo 5. En este glosario, no se encontró equivalente exacto en español para ninguno de los ejemplos de necesidades informativas terminológicas que se plantearon en el segundo capítulo. Lo más cercano fue el caso de *safety*, que aparecía junto con otras palabras

para crear un término en particular. Por ejemplo, «evaluación de la seguridad» aparecía como equivalente de *safety assessment* (314), mientras que «protección y seguridad» aparecía como equivalente de *protection and safety* (324). A partir de esto, se podría asumir que *safety* se traduce como «seguridad» de acuerdo con esta publicación. No obstante, no coincide con lo indicado por el *Glosario de seguridad tecnológica del OIEA*. Por otra parte, no se descarta que se puedan encontrar soluciones para el resto de términos que representaron un reto terminológico. En los siguientes párrafos se evaluarán la utilidad y la confiabilidad de este recurso con base en los parámetros incluidos en las fichas descriptivas.

Descripción general, autoría y contenido

Encontrar la información relacionada con este glosario requirió algunos pasos adicionales. Como se puede ver en la captura de pantalla de los resultados de la búsqueda, esta fuente se titulaba «glosario – IAEA Publications» y su dirección electrónica se encuentra dentro del dominio del sitio web del OIEA. Sin embargo, al abrir el archivo, en la primera página, se lee únicamente la palabra «Glosario» y empieza a listar las páginas a partir de la 305. Esto hace suponer que pertenece a un documento más grande, pero inicialmente no se encuentran indicios de la fuente bibliográfica de origen. Es hasta el final de las 68 páginas que se encuentra un código ISBN, el cual se busca en Google y se obtiene como resultado las *Normas básicas internacionales*, que es la publicación número 115 de la Colección Seguridad del OIEA. Al momento de realizar la investigación, el documento no estaba disponible para su descarga en la página oficial del organismo. Sin embargo, en otro resultado de la búsqueda, en la página de la Organización Internacional del Trabajo, fue posible encontrar el enlace de descarga para obtener más información sobre este texto y poder descargarlo. Gracias a este proceso de búsqueda fue posible obtener más detalles que permitieron evaluar esta fuente bibliográfica.

El documento *Normas básicas internacionales* en general establece los requisitos para la protección contra los riesgos que pueda representar la exposición a la radiación y a las fuentes radiactivas. Este documento fue publicado por el OIEA en el año 1997. Su fecha de publicación lo convierte en uno de los documentos más antiguos que arrojó el proceso de documentación. Se considera desde un inicio que esta publicación está bastante desactualizada si se compara con el resto de información que se había encontrado en las búsquedas anteriores. Dentro de esta publicación, se encuentra el glosario que se obtuvo como resultado de la fase de búsqueda de glosarios bilingües, con el cual se podrían solventar necesidades informativas terminológicas. Los términos en español aparecen en orden alfabético, con su equivalente en inglés entre paréntesis y su definición en español. Además de esa sección, se encuentra una lista de normas internacionales relacionadas con la seguridad de las fuentes radiactivas en la medicina y el comercio en general. Esto último también podría servir para solventar necesidades informativas temáticas; una de las preguntas planteadas en el segundo capítulo de esta investigación se refería a cuál era el uso que se le daba a las fuentes radiactivas, respuesta que puede brindar esta publicación. Puesto que el documento *Normas básicas internacionales* no es reciente, otra utilidad podría ser la de ofrecer un vistazo al contexto que precedió la creación de guías como la de *Security of Radioactive Sources*.

Compatibilidad, funcionabilidad, navegabilidad y diseño

Esta publicación se encuentra en formato PDF, cuyas ventajas ya han sido comentadas en fuentes documentales anteriores. Mediante la página oficial del OIEA, se descubrió que esta guía también cuenta con versiones en árabe, chino, francés, inglés y ruso. La versión en inglés podría ser útil, pero dada la antigüedad, se evitaría su uso a menos de que fuera para un caso muy particular. Se consideró que la organización de los contenidos era lógica y el menú permitía

desplazarse fácilmente a diferentes secciones del documento. A pesar de que el texto se puede leer claramente, luce como si fuera escaneado. Si se compara con otras publicaciones más recientes del OIEA, se notará que es menos nítido y hasta aparenta ser un texto más antiguo. Aun así, si bien la nitidez del texto es un aspecto mejorable, no se consideró que le restara valor a la publicación y, por ende, su glosario, desde el punto de vista del diseño.

Pertinencia y conclusiones

En conclusión, a pesar de ser un glosario que fue creado por el OIEA para una de sus publicaciones, se considera que su antigüedad le resta valor desde el punto de vista documental. El primer resultado de esta fase de búsquedas había ofrecido una publicación que lo aventajaba por diez años, lo cual es un número considerable. No obstante, a pesar de las múltiples características en contra de su fiabilidad como fuente documental, si se extiende el análisis al documento *Normas básicas internacionales* en su totalidad, más que solo su glosario, es la primera fuente capaz de ofrecer soluciones para las tres necesidades informativas planteadas. Su glosario proporciona terminología y su contenido solventa vacíos sobre el tema; además, la versión en inglés de esta colección aparece citada en la guía *Security of Radioactive Sources*, por lo que contar con una versión en español puede ayudar a definir la manera en la que se remitirá a esta publicación. Se considera que este es uno de los aspectos de mayor relevancia para la traducción, pues otras fuentes bibliográficas más recientes se consideran las idóneas para cubrir necesidades informativas terminológicas y temáticas.

3.3. Búsqueda de información sobre la materia

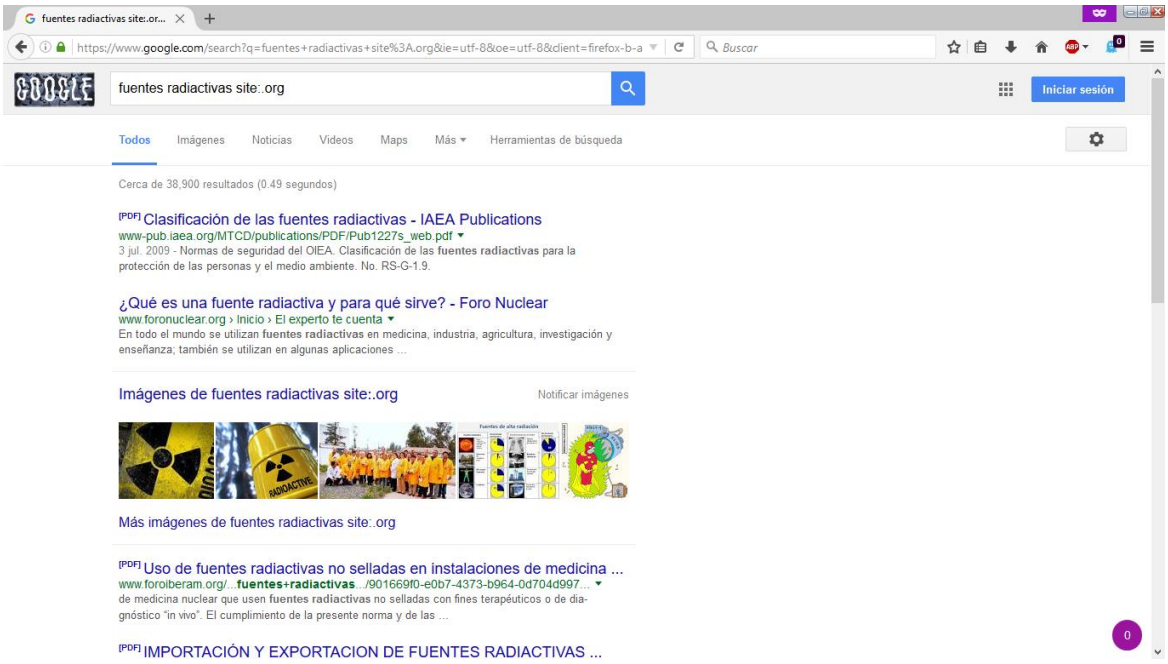
En esta fase se recolectaron y analizaron recursos que permitieran solventar las necesidades informativas temáticas identificadas en la guía *Security of Radioactive Sources*, paso fundamental para entender el texto original y así poder transmitir la información en la

traducción. Al igual que en la búsqueda de recursos de terminología, se utilizó la función avanzada de Google. Para recrear el proceso de búsqueda que realizaría un traductor, se decidió buscar las frases comentadas en la sección de necesidades informativas temáticas del segundo capítulo y configurar la búsqueda mediante el operador «site:.org» para que el sitio o dominio perteneciera a alguna organización u organismo sin fines de lucro que pudiera ofrecer recursos o fuentes oficiales. Esta medida se tomó para conocer el contexto institucional en el cual se desarrollarían los temas analizados. Se descartó el uso de búsqueda de frases exactas para extender el alcance de los resultados. Tal y como se procedió en la sección anterior, se agregará una captura de pantalla con los resultados de la búsqueda y se analizarán dos de ellos.

3.3.1. Fuentes radiactivas

En el capítulo anterior se plantearon diferentes preguntas relacionadas con un tema general en particular: las fuentes radiactivas. Por esta razón, se considera útil que el traductor cuente con un conocimiento general del tema que permea todo el texto que se está traduciendo. Para ello, se ingresó en Google la frase «fuentes radiactivas site:.org». En la imagen siguiente se presentan los resultados obtenidos:

Imagen 5. Fuentes radiactivas en Google



3.3.1.1. *Clasificación de las fuentes radiactivas*

Descripción general, autoría y contenido

El primer resultado que se obtuvo es la publicación titulada *Clasificación de las fuentes radiactivas*, cuya ficha se puede encontrar en el anexo 6. Este es un documento del OIEA publicado en el 2009 que brinda información detallada, a modo de guía, sobre la clasificación de las fuentes radiactivas con base en el riesgo que puedan representar para la salud; esto con el propósito de que los Estados, las autoridades pertinentes y los operadores puedan hacer sus propias clasificaciones. En la sección donde se describe el alcance de la publicación, se indica que se abordan las fuentes radiactivas que «se emplean en la industria, la medicina, la agricultura, la investigación y la enseñanza» (3). Gran parte de esta publicación está compuesta por cuadros donde se indica el tipo de fuente radiactiva, el tipo de material radiactivo, el nivel de actividad, el nivel de riesgo, entre otros aspectos. Varios de estos cuadros están citados en la

guía *Security of Radiactive Sources*. El documento titulado *Clasificación de las fuentes radiactivas* proporciona la versión en español de los mismos y se convierte en un texto de suma utilidad para la traducción de la guía.

Otro aspecto de contenido que se considera de suma utilidad es que esta publicación distingue el uso de *shall* y *should*. En el segundo capítulo de esta investigación, como parte de las necesidades informativas temáticas, se comentó el reto traductológico que suponía el uso de *should* en toda la guía *Security of Radioactive Sources*. En una sección introductoria del documento *Clasificación de las fuentes radiactivas*, la cual se titula «Normas de seguridad del OIEA», se explica que las normas del OIEA se dividen en las siguientes cuatro categorías: Nociones fundamentales de seguridad, Requisitos de seguridad y Guías de seguridad (s. pag.). Lo expuesto en relación con las últimas dos es de suma importancia para entender la intención que persigue cada una de estas categorías. Sobre los «Requisitos de seguridad» se detalla lo siguiente:

> Establecen los requisitos que deben cumplirse para garantizar la protección de la población y el medio ambiente, tanto en el presente como en el futuro. Estos requisitos, en cuya formulación se emplea generalmente la forma deberá(n) o expresiones como "habrá que", "hay que", "habrá de", "se deberá" (en inglés "shall"), se rigen por los objetivos, conceptos y principios de las Nociones fundamentales de seguridad (…). Las publicaciones de Requisitos de seguridad están redactadas en forma de textos reglamentarios, lo cual permite su incorporación en leyes y reglamentos nacionales. (s. pag.)

En contraposición a este enunciado, la descripción de las «Guías de seguridad» indica lo siguiente:

> [Las guías] ofrecen recomendaciones y orientación sobre cómo cumplir los requisitos de seguridad. En la formulación de las recomendaciones de las Guías de seguridad se emplea generalmente la forma debería(n) o expresiones como “conviene”, “se recomienda”, “es aconsejable” (en inglés “should”). Se recomienda adoptar las medidas señaladas u otras medidas equivalentes (...). Cada publicación de Requisitos de seguridad está complementada por varias Guías de seguridad, que se pueden utilizar en la elaboración de guías nacionales de reglamentación. (s. pag.)

Estas dos citas resuelven la incógnita sobre la razón del uso de *should* dentro de la guía. Desde el punto de vista temático, la *Clasificación de las fuentes radiactivas* aclaró por qué *should* reflejaba el propósito de las guías de seguridad en contraposición a los requisitos de seguridad, sobre los cuales no se había encontrado información específica hasta este punto de las búsquedas y, por lo tanto, no se tenía punto de comparación. Desde la perspectiva terminológica, se obtuvieron cuatro formas de traducir dicho modal, de manera que sea acorde con el propósito del resto de guías de esta colección del OIEA.

Compatibilidad, funcionabilidad, navegabilidad y diseño

Su formato es PDF, cuyas ventajas ya han sido comentadas en fuentes documentales anteriores. Mediante una búsqueda en Google similar a la que se empleó con el *Glosario de seguridad tecnológica del OIEA*, se encontró una página también titulada «Clasificación de las fuentes radiactivas», en la cual se descubrió que esta guía también cuenta con versiones en árabe, chino, francés, inglés y ruso. Contar con las versiones en inglés y español podría ayudar a resolver otras necesidades terminológicas que se presenten en la traducción. Se consideró que la organización de los contenidos era lógica. Los títulos y subtítulos cuentan con marcadores; sin embargo, al momento de realizar esta investigación, los mismos no eran funcionales pues,

al hacer clic en ellos, el usuario no era llevado a la parte del documento donde se encontraba el título o subtítulo que se buscaba, como sí sucedió con las otras publicaciones del OIEA que se encontraron para este trabajo. En cuanto a diseño, se empezó a notar una tendencia en comparación con el resto de publicaciones del OIEA: los colores empleados (blanco y negro, salvo la portada y la tipografía); todos estos aspectos se consideraron apropiados y funcionales.

Pertinencia y conclusiones

En conclusión, el documento *Clasificación de las fuentes radiactivas* es otro recurso de suma utilidad y fiabilidad para la traducción de la guía *Security of Radioactive Sources*. En los párrafos anteriores se comentó que es una fuente documental que tiene el potencial de resolver diferentes necesidades informativas temáticas y terminológicas. Además, diferentes cuadros de la guía que se está traduciendo fueron tomados de este documento, por lo que también su versión en inglés aparece en la sección de «Referencias» de la guía en estudio. Esto hace que resuelva también necesidades informativas referenciales y se convierta en otra fuente bibliográfica con capacidad de resolver problemas traductológicos pertenecientes a las tres necesidades informativas planteadas para este trabajo. A diferencia de la *Normas básicas internacionales*, esta publicación es del 2009, mismo año de publicación de la guía *Security of Radioactive Sources*, lo cual le agrega aún más valor desde el punto de vista documental.

3.3.1.2. «¿Qué es una fuente radiactiva y para qué sirve?»

Descripción general, autoría y contenido

El segundo resultado que se obtuvo fue una página del Foro de la Industria Nuclear Española, titulada «¿Qué es una fuente radiactiva y para qué sirve?» (ver ficha descriptiva en el anexo 7), la cual dedica algunos párrafos a una explicación general sobre las fuentes radiactivas. Esta explicación abarca los campos en los cuales se utilizan (medicina, industria, agricultura,

investigación, enseñanza y ejército), las maneras de almacenarlas, su registro, la infraestructura legal que las rige y, al final, añade un apartado para detallar qué se debe hacer con una fuente que ha sido abandonada. Esta información es parte de una sección de la página llamada «El experto te cuenta», donde se incluyen enlaces a otros temas relacionados, como las aplicaciones de la tecnología nuclear, la diferencia entre la fisión y fusión nuclear, últimos avances en el uso de la energía nuclear, entre muchos otros temas de interés. En los diferentes enlaces se notó que la información se presentaba de manera informativa, sencilla y clara, dirigida a una audiencia amplia que no fuera experta en la materia. Además de «El experto te cuenta», existen otras dos secciones relacionadas que se titulan «Enviar consulta al experto» y «Consultas al experto». En la primera existe un formulario mediante el cual se pueden enviar preguntas; por medio de la segunda, se puede tener acceso a las preguntas hechas por otras personas con sus respectivas respuestas. En la página de inicio también fue posible encontrar enlaces a sus publicaciones, recursos educativos y enlaces externos a organismos nacionales e internacionales que se relacionan con la energía nuclear, incluido el OIEA.

En un enlace titulado «Sobre nosotros», se indica que el Foro de la Industria Nuclear Española es una asociación que agrupa a empresas españolas que hacen usos pacíficos de la energía nuclear y que persiguen objetivos comunes en términos de seguridad y fiabilidad. En esta sección, también es posible ver su misión, visión, valores, objetivos, actividades y socios; sobre lo último, se puede encontrar una lista de todas las empresas afiliadas con enlaces a sus respectivos sitios web. Además, también cuenta con un formulario para contactar al foro. En su conjunto, la manera de presentar la información dota de credibilidad a los contenidos mostrados. Otro aspecto que brinda credibilidad es que, al menos en la sección de «El experto te cuenta», se revela que los contenidos fueron creados y actualizados recientemente; según los enlaces que

se visitaron, se indican fechas que van desde el 2014 hasta el 2016. En los títulos de cada enlace se especifica la fecha en la que se publicó el enlace específico y la fecha en la que se actualizó, en caso de que haya sido actualizado. Esto brinda bastante fiabilidad pues, no solo se cuenta con fecha de publicación, sino también, fecha de actualización. En general las publicaciones son bastante recientes y todas han sido actualizadas.

Compatibilidad, funcionabilidad, navegabilidad y diseño

Su formato HTML permite desplazarse fácilmente a los distintos enlaces y secciones. Como se comentó anteriormente para el diccionario de la REMM, un aspecto en su contra es que depende de una conexión activa a internet y que se limita la funcionalidad de imprimir a un formato que sea amigable con el usuario. Se considera que los contenidos se presentan de manera lógica y que los diferentes menús y enlaces son funcionales. Es fácil desplazarse dentro del sitio web y no se encontraron enlaces rotos. El diseño es muy llamativo y amigable con el usuario pues el empleo de colores, animaciones y tipografía se consideraron atractivos y bien seleccionados. Se considera que, en parte, esto responde a que la página luce como un lugar de difusión de la información para audiencias que no necesariamente sean expertas en la materia.

Pertinencia y conclusiones

En conclusión, además de la información obtenida en un inicio mediante la búsqueda de Google, se considera que el sitio web del Foro de la Industria Nuclear Española proporciona información valiosa y fácil de entender para un traductor que no se haya enfrentado anteriormente a la radiactividad como área temática. El contenido de esta página podría llenar el vacío general de conocimiento sobre el tema sin recurrir a largos documentos con datos más técnicos y exhaustivos. Por otra parte, el foro como tal ofrece bastante credibilidad y se considera un buen punto de inicio para la solvencia de las necesidades informativas temáticas.

En cuanto al resto de las necesidades, si bien se puede obtener terminología útil, dado que el proceso de documentación ha revelado lo robusto del sistema de publicaciones del OIEA, se preferiría buscar los términos y sus equivalentes en español en textos publicados por el mismo organismo que elaboró la guía *Security of Radioactive Sources*. Por otra parte, el sitio web en análisis no brinda directamente soluciones a las necesidades informativas referenciales presentes en la guía.

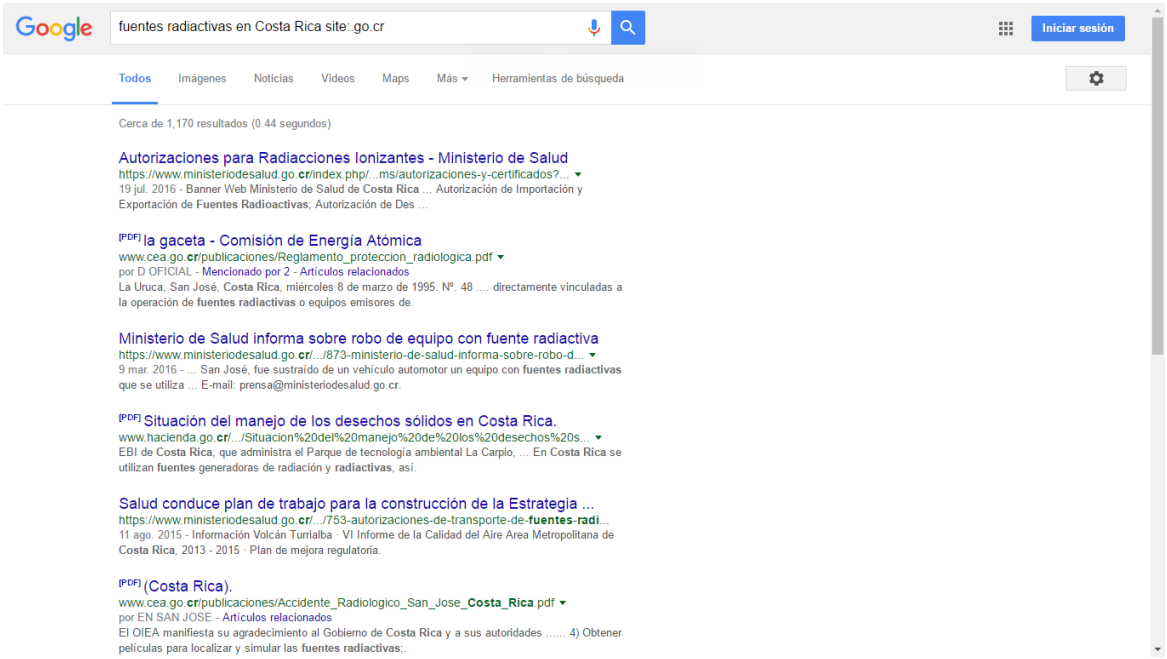
Cabe destacar el factor interactivo de este sitio web. En el aparato crítico de este trabajo, se comentó que una de las etapas de búsqueda propuestas por Merlo Vega era la búsqueda de especialistas en la materia. Si bien en la metodología de esta investigación se descartó realizar esa etapa, el sitio del Foro de la Industria Nuclear Española le permitiría a un traductor realizar consultas directas con expertos en la materia.

3.3.2. Fuentes radiactivas en Costa Rica

Entre las preguntas que se plantearon sobre las fuentes radiactivas, se incluía la duda sobre la existencia de las fuentes radiactivas en Costa Rica y su ubicación. Aunque la traducción iba a estar dirigida a un público hispanohablante en general, sería útil para el traductor obtener información sobre el estado de las fuentes en su propio país pues, por una parte, se considera que se podría entender mejor la relevancia de una guía de seguridad de fuentes radiactivas al ponerla en el contexto del traductor; por otra parte, si bien esta investigación se centra en la utilización de recursos electrónicos como fuentes documentales, las páginas web que pertenezcan a instituciones costarricenses podrían ofrecer al traductor contactos en su propio en caso de que sea necesario consultar con expertos en la materia. Para cumplir con el propósito de esta parte de la investigación, la búsqueda se limitó a sitios gubernamentales costarricenses

mediante el operador «site:.go.cr». Con las palabras «fuentes radiactivas en Costa Rica site:.go.cr», se obtuvieron los resultados que se pueden observar en la siguiente imagen:

Imagen 6. Fuentes radiactivas en Costa Rica



A pesar de que las palabras que se utilizaron en el buscador fueron las que arrojaron los resultados más provechosos para esta investigación, en este caso, la metodología se modificará pues el primer resultado obtenido no ofrece directamente información sobre las fuentes radiactivas. Se trata de una página oficial del Ministerio de Salud titulada «Autorizaciones y certificaciones», en concreto, la sección llamada «Radiaciones ionizantes», la cual ofrece enlaces a leyes, formularios y guías para la elaboración de certificados y manuales de procedimientos relacionados con material radiactivo. Por sí misma, la página no ofrece contenido; sin embargo, da a conocer que ese ministerio es el encargado de regular lo relacionado con las fuentes radiactivas; además, al final de la página se ofrece información de

contacto del ministerio. Se creó el anexo 8 con la ficha descriptiva pues, como se mencionó en la introducción de esta etapa de búsquedas, futuros traductores podrían requerir información sobre los diferentes formularios y leyes que se ofrecen en este enlace. En los próximos párrafos se analizarán el segundo y el tercer resultado de la búsqueda.

3.3.2.1. *Reglamento sobre protección contra las radiaciones ionizantes*

Descripción general, autoría y contenido

El segundo resultado que se obtuvo fue el Decreto No 24037-S, titulado *Reglamento sobre protección contra las radiaciones ionizantes* (ver ficha descriptiva en el anexo 9). En este decreto, se brinda información sobre la autoridad encargada de las normas, los criterios técnicos y los permisos relacionados con las radiaciones ionizantes. Se confirma que el Ministerio de Salud es la autoridad reguladora; sin embargo, esta página web indica que la autoridad se ejerce mediante el Programa de Control de Radiaciones de la Dirección de Protección al Ambiente Humano (s. pag.). Después, se ofrecen algunas definiciones que se utilizarán en el reglamento y que podrían ser de utilidad para las preguntas de carácter terminológico.

Más adelante, los contenidos se dividen en capítulos, los cuales a su vez contienen diferentes artículos. Estos brindan detalles sobre temas como los siguientes:

i. Tipos de instalaciones donde se almacenarán materiales o equipos que utilicen radiación y los requisitos que deberán cumplir
ii. Obligaciones de los titulares de licencias para realizar actividades que involucren radiación
iii. Obligaciones de los operadores de fuentes radiactivas
iv. Transporte, importación y exportación de fuentes radiactivas
v. Transferencia de títulos, instalaciones, fuentes o equipos

vi. Inspecciones

vii. Áreas de trabajo

viii. Límites de dosis

ix. Desechos radiactivos

x. Protección radiológica en la práctica médica

xi. Emergencias radiológicas

xii. Sanciones

Esos capítulos darían respuesta a otras preguntas que se plantearon en el Capítulo 2 de esta investigación, tales como las relacionadas con la definición de radiactividad, sus usos y la ubicación de las fuentes radiactivas, al menos dentro del ámbito costarricense. Para ilustrar una de las respuestas, el artículo 8, en la sección «a», lista diferentes instalaciones de Tipo I donde se pueden ubicar fuentes radiactivas, por ejemplo, las siguientes:

1. Instalaciones médicas en donde se realicen prácticas de terapia, mediante radiaciones ionizantes. (2)
2. Instalaciones médicas en donde se realicen prácticas de diagnóstico con rayos X. (3)
3. Instalaciones médicas en donde se manipule o trate material radiactivo, en forma de fuentes no selladas, para uso en terapia o diagnóstico con técnicas "in vivo". (4)

Estos ejemplos revelan el tipo de instalaciones médicas donde es posible encontrar fuentes radiactivas. A partir de esto es posible entender que los médicos y los pacientes son algunas de las personas que podrían estar expuestas en primera instancia a una eventual emergencia radiológica. Aparte de esta información, se considera que uno de los puntos más valiosos de este decreto es reconocer que en el país existe reglamentación para el uso de las fuentes radiactivas. Se entiende, entonces, que la protección de las fuentes deja de ser un tema general para

convertirse en uno debidamente regulado en el plano jurídico. La guía *Security of Radioactive Sources* serviría de base para la redacción de reglamentos como este, algo que no se había descubierto en búsquedas anteriores. En los siguientes párrafos se evaluará la fiabilidad y la utilidad de este decreto como fuente documental.

Este es un decreto publicado en el año 1995 por el Ministerio de Salud Costa Rica en *La Gaceta*, el diario oficial del Estado. Se considera que esta versión es antigua pues al momento de realizar la investigación cumplía más de veinte años de haber sido publicado; sin embargo, en su primera página se indica que esta sustituye una versión más antigua, publicada en 1980. Mediante una búsqueda en Google, fue posible descubrir que, en la página del Ministerio de Salud, se encuentra la última versión de este reglamento, el cual data del 2009. Se esperaría que varias partes del contenido hayan sido actualizadas. La afinidad con la guía que se está traduciendo es considerable, dado que, como se mencionó en el párrafo anterior, este es el tipo de reglamentos para el cual serviría de base la guía.

Compatibilidad, funcionabilidad, navegabilidad y diseño

Su formato es PDF, con las ventajas mencionadas en fuentes documentales anteriores, y no se encontraron versiones en otras lenguas. Esto es entendible dado que es un decreto creado para Costa Rica y traducirlo a otro idioma resulta innecesario a menos que fuera por una razón muy específica o que lo requiriera un organismo internacional. La estructura de los contenidos se considera apropiada para un reglamento, pues se divide en capítulos, secciones y artículos. El texto no cuenta con un menú de marcadores de contenidos funcional con el cual se pueda desplazar rápidamente a capítulos específicos del reglamento. Se considera que su diseño, los colores empleados (blanco y negro) y la tipografía son los adecuados para un decreto oficial.

Pertinencia y conclusiones

En conclusión, este decreto solventó varias de las necesidades informativas temáticas planteadas en relación con el uso de las fuentes radiactivas en Costa Rica. Además, sirvió para responder a otras preguntas que se habían hecho en la fase semasiológica de la documentación con respecto a la radiactividad en general, la ubicación de las fuentes radiactivas y su uso. Podría eventualmente solventar también algunas necesidades informativas terminológicas, pero en aspectos de fiabilidad, es preferible contar con fuentes documentales más recientes. Los puntos negativos más notables fueron su antigüedad y la falta de un menú de marcadores funcional. Aun así, en un ambiente real de traducción, haber encontrado el decreto de 1995 podría llevar a buscar la versión más reciente del decreto y utilizarla como base para tomar decisiones traductológicas.

3.3.2.2. «Ministerio de Salud informa sobre robo de equipo con fuente radiactiva»

Descripción general, autoría y contenido

El tercer resultado fue un comunicado de prensa del Ministerio de Salud titulado «Ministerio de Salud informa sobre robo de equipo con fuente radiactiva» (ver ficha descriptiva en el anexo 10) donde se informa sobre el robo de un densímetro nuclear, el cual se utiliza en la medición de la densidad y la humedad de los suelos. En el segundo capítulo de esta investigación se consideró que una de las necesidades informativas temáticas era la amenaza a las fuentes radiactivas. En este caso particular, se aclara lo siguiente:

> Dicho equipo no representa un riesgo inminente a la salud, pero si es manipulado por personas inexpertas o sin capacitación sí podrían verse afectadas, por tratarse de una fuente radiactiva. (s. pag.)

Aunque en este caso el robo no representó una amenaza mayor, se pone de manifiesto el peligro que podría representar que personas sin conocimiento manipulen equipos con fuentes

radiactivas. Más adelante, el comunicado hace mención particular a «las empresas que manipulan residuos metálicos o electrónicos y establecimientos dedicados a la compra y venta» (s. pag.), los cuales sin proponérselo podrían estar expuestos a materiales radiactivos. La mayoría de personas no podrían identificar un equipo que utilice este tipo de materiales, incluidos los traductores, por lo que otra característica relevante de este comunicado como fuente de información es que brinda un par de imágenes para poder identificar los equipos. Finalmente, el otro aspecto que se consideró de utilidad fue que se indican los organismos a los que se podría contactar en caso de encontrarse con estos equipos, los cuales se listan a continuación:

a. Policía local
b. 911
c. Dirección de Inteligencia y Seguridad (DIS)
d. Unidad Especial Intervención del Ministerio de la Presidencia
e. Ministerio de Salud

Además, se indican los números de teléfono de cada entidad. Como se mencionó en casos anteriores, si bien la búsqueda de especialistas quedó fuera del alcance de esta investigación, los traductores podrían obtener de este comunicado algunos organismos involucrados en la protección de fuentes radiactivas a los que podrían acudir para resolver dudas con expertos.

Como fruto del proceso de documentación que se ha llevado a cabo, y mediante el análisis del *Reglamento sobre protección contra las radiaciones ionizantes*, en este punto de la investigación se conoce que el Ministerio de Salud representa la principal autoridad en Costa Rica en materia de fuentes radiactivas, lo que hace confiar en la veracidad de esta fuente documental. El comunicado se publicó el 8 de marzo del 2016, por lo que destaca la importancia

de proteger las fuentes radiactivas en la realidad. Se considera que el comunicado es afín con la guía *Security of Radioactive Sources* porque muestra cómo las recomendaciones que esta ofrece tienen utilidad en la realidad. En esta página también se ofrecen enlaces a otras noticias y notas de prensa publicadas por el Ministerio de Salud, aunque la mayoría no se relacionan con fuentes radiactivas.

Compatibilidad, funcionabilidad, navegabilidad y diseño

Su formato es HTML, con las ventajas y desventajas comentadas en los análisis de recursos documentales encontrados anteriormente. No se encontró una versión en inglés que se correspondiera con el texto original para encontrar términos equivalentes en los dos idiomas. En los pocos párrafos, se sigue una estructura lógica de la información. Los menús con los diferentes enlaces a páginas dentro del sitio del Ministerio de Salud funcionaban; no obstante, como se mencionó en el párrafo anterior, no necesariamente llevaban a enlaces relacionados con el tema en estudio. Su diseño, los colores y la tipografía se consideraron útiles y atractivos; incluir imágenes no sólo ayudó a ilustrar los equipos robados, sino que hizo que la página fuera más llamativa.

Pertinencia y conclusiones

Como conclusión, esta página web cumplió con al menos una de las necesidades informativas temáticas, las amenazas a las fuentes radiactivas, aunque de manera muy superficial. Se podría decir que se consiguió un ejemplo de amenaza más que brindar un amplio conocimiento sobre las mismas. Entre los aspectos a destacar se encuentran su autoría y actualidad, las cuales se consideraron bastante apropiadas y fiables como fuente de información. Se considera que su mayor debilidad consiste en no ofrecer enlaces a noticias relacionadas con fuentes radiactivas; para hacerlo, habría que realizar una búsqueda más exhaustiva. Esto es

entendible dado que es un sitio que abarca todo lo que compete al Ministerio de Salud, pero para los objetivos de esta investigación, se buscaría un sitio más especializado en el tema de la radiactividad.

3.4. Búsqueda de textos paralelos con versiones en inglés y español

En la siguiente fase de documentación, se procedió a buscar textos paralelos. Como se mencionó en la metodología, en esta etapa no se empleó un motor de búsqueda en línea puesto que, al inicio del proceso de documentación, se encontró la lista completa de documentos que pertenecen a la Colección de Seguridad Nuclear del OIEA, los cuales se listan en la página «Nuclear Security Series Publications». Por asuntos de espacio y para obtener los resultados que mejor pudieran satisfacer las necesidades informativas planteadas, primero se eligió un documento de cada una de las cuatro categorías de publicación listadas, las cuales se dividían en «Fundamentals», «Recommendations», «Implementing Guides» y «Technical Guidance». De cada una, se eligió la publicación más reciente que contara con versión en inglés y en español. A continuación se listan las fuentes documentales analizadas en este apartado:

i. *Objective and Essential Elements of a State's Nuclear Security Regime*
ii. *Nuclear Security Recommendations on Radioactive Material and Associated Facilities*
iii. *Security in the Transport of Radioactive Material*
iv. *Computer Security at Nuclear Facilities*

En los próximos párrafos se analizará cada una de ellas y se indicará el anexo donde se encuentra su respectiva ficha descriptiva. No obstante, puesto que todas las fuentes documentales fueron publicadas por el OIEA y pertenecen a la misma colección, se dedicará un segmento inicial a analizar los aspectos que comparten las cuatro con base en los parámetros incluidos en las fichas descriptivas. En primer lugar, se brindará un resumen del contenido de

cada publicación; en segundo lugar, de estar presentes, se comentarán aspectos particulares de cada una.

3.4.1. Criterios compartidos

Descripción general, autoría y contenido

Como se puede ver en las fichas descriptivas que se encuentran en los anexos 10-18, todas las publicaciones analizadas en este apartado compartían ciertos criterios, por lo que se optó por unificarlos en esta sección para evitar la repetición. En primer lugar, todas tienen como autor al Organismo Internacional de Energía Atómica. Salvo el documento titulado *Computer Security at Nuclear Facilities*, que aborda la ciberseguridad aplicada a la protección de fuentes en instalaciones nucleares, todas las demás se relacionan de cierta manera con la guía *Security of Radioactive Sources*. Este aspecto hace que la mayoría de las fuentes analizadas ayuden, al menos, a solventar ciertas necesidades informativas terminológicas y temáticas. Finalmente, aunque no todas las publicaciones aparecen citadas en la guía que se está traduciendo, todas revelaron la manera en la que se presentan las citas y la sección de referencias de acuerdo con la colección de seguridad.

Compatibilidad, funcionabilidad, navegabilidad y diseño

En cuanto al formato de los documentos, todos los textos se encuentran en formato PDF, con las ventajas mencionadas en apartados anteriores. La estructura y la organización de los contenidos se consideraron lógicas y presentaban la información de forma fluida. Finalmente, puesto que todas pertenecen a una misma colección, los aspectos de diseño, combinación de colores y tipografía eran compartidos; estos criterios dejaban ver lo estandarizado del diseño utilizado para esta colección de seguridad, lo cual caracteriza a los textos de tipo técnico. Por parte de esta colección de seguridad, esto también reveló el criterio de uniformidad que

caracteriza a las publicaciones del OIEA mediante el uso de un estilo definido. En los siguientes párrafos se presentarán los aspectos particulares de cada publicación, especialmente en relación con el contenido y la posibilidad de resolver los diferentes tipos de necesidades que planteó la traducción de la guía *Security of Radioactive Sources*.

3.4.2. *Objective and Essential Elements of a State's Nuclear Security Regime*

El único documento que formaba parte de la categoría «Fundamentals» se titula *Objective and Essential Elements of a State's Nuclear Security Regime*, publicado en el 2013 (ver ficha descriptiva en el anexo 11). Su versión en español se titula *Objetivo y elementos esenciales del régimen de seguridad física nuclear de un Estado* (ver ficha descriptiva en el anexo 12) y fue publicada en el 2014. En este documento se presentan el objetivo y los elementos esenciales del régimen de seguridad física nuclear que servirán de base para el resto de las publicaciones; por ello, se considera «la publicación principal de la Colección de Seguridad Física Nuclear el OIEA» (2). Este pequeño texto (suma 32 páginas en total, sin contar la introducción), se divide en tres secciones, las cuales se detallan a continuación:

a. Sección 1: «Visión general de los antecedentes, la finalidad, el ámbito de aplicación y la estructura del documento (4)
b. Sección 2: «Objetivo del régimen de seguridad física nuclear de un Estado» (4)
c. Sección 3: «Conjunto de elementos esenciales del régimen de seguridad física nuclear de un Estado» (4)

De estas tres secciones, la última es la más extensa con siete de las doce páginas de contenido. Los elementos esenciales abarcan, por ejemplo, la responsabilidad del Estado en la protección de las fuentes radiactivas, la determinación y la definición de las responsabilidades en materia de seguridad nuclear, el marco legislativo y regulador, el transporte de materiales

radiactivos, entre otros. De contar con el tiempo, se considera que esta publicación se podría leer antes de realizar la traducción para tener un conocimiento más amplio de los principios que rigen la guía *Security of Radioactive Sources* y familiarizarse con el vocabulario y el estilo de redacción.

Si bien la mayoría de los parámetros de evaluación coinciden con los del resto de publicaciones de la Colección de Seguridad Nuclear, la versión en español de este documento carece de un menú de marcadores funcional; en la versión en inglés es posible saltar a las diferentes secciones del documento con sólo hacer clic en los marcadores que, según el lector de PDF con el que se cuente, aparecen a mano izquierda del documento. En la versión en español sólo existen dos marcadores, uno llamado «_GoBack», que lleva a la introducción del texto, y otro llamado «tw4winUpto» que lleva a la página 14 de definiciones. Se considera que fue un error de paginación y que debería ser reparado para ser plenamente funcional. Por otra parte, esta publicación no está citada en la guía *Security of Radioactive Sources* y carece de una sección de Referencias, por lo que no ayuda a solventar necesidades informativas referenciales.

3.4.3. *Nuclear Security Recommendations on Radioactive Material and Associated Facilities*

Como parte de las fuentes incluidas en «Recommendations», se analizará la publicación titulada *Nuclear Security Recommendations on Radioactive Material and Associated Facilities*, publicada en el 2011 (ver ficha descriptiva en el anexo 13). Su título en español es *Recomendaciones de seguridad física nuclear sobre materiales radiactivos e instalaciones conexas*, versión publicada en el 2012 (ver ficha descriptiva en el anexo 14). En su introducción, se indica que este documento está a un segundo nivel de jerarquía dentro de la Nuclear Security Series, por debajo de las «Nociones fundamentales de seguridad física nuclear». Sobre esta característica, se indica lo siguiente:

> [En las Recomendaciones] se analizan más a fondo los elementos esenciales de la seguridad física nuclear y se expone el consenso internacional sobre las medidas que deberían adoptar los Estados para aplicar esos elementos. (1)

Para lograr lo ahí expuesto, esta publicación propone objetivos y elementos que deberían tener los regímenes estatales en lo relacionado a materiales radiactivos, así como las instalaciones que los almacenen y las actividades que se lleven a cabo con ellos. Al hablar de elementos, se refiere, por ejemplo, a la manera de asignar responsabilidades, la existencia de un marco reglamentario, el sistema de cooperación internacional, la determinación y evaluación de las amenazas, entre otros puntos. Más adelante, comparte otras recomendaciones relacionadas con la clasificación de las fuentes, la evaluación de las amenazas y el sistema de seguridad física, entre otros temas que también son mencionados en la guía *Security of Radioactive Sources* y que podrían ser fuente de terminología especializada útil para la traducción.

Si bien esta publicación no aparece citada en la guía que se está traduciendo, sí cuenta con una sección de referencias que el traductor puede utilizar como base para tomar decisiones de índole referencial. En primer lugar, aclara que la manera de presentar las citas se mantiene en las versiones en inglés y en español, posiblemente en aras de uniformar el estilo de documentación. En segundo lugar, también resuelve necesidades específicas. Por ejemplo, uno de los documentos citados en la guía *Security of Radioactive Sources* y en el documento *Recomendaciones de seguridad física nuclear sobre materiales radiactivos e instalaciones conexas* es la *International Convention for the Suppression of Acts of Nuclear Terrorism*. En la versión en español, esta aparece como el *Convenio internacional para la represión de los actos de terrorismo nuclear* y se ofrece la manera particular en la que el OIEA presenta la referencia en español.

3.4.4. *Security in the Transport of Radioactive Material*

Como parte de las «Implementig Guides», se analizará la publicación titulada *Security in the Transport of Radioactive Material*, publicada en el 2008 (ver ficha descriptiva en el anexo 15). Su título en español es *La seguridad en el transporte de materiales radiactivos*, versión que se publicó en el 2013, cinco años después de la versión original en inglés (ver ficha descriptiva en el anexo 16). Este documento aborda la protección de los materiales radiactivos durante su fase de transporte. Se proporcionan las orientaciones para el diseño y la evaluación de las medidas de protección, así como para el establecimiento de niveles de seguridad. Mediante esta guía fue posible solventar necesidades informativas terminológicas como las del uso de *safety* y *security* en español. Puesto que su versión en español es de las más recientes de esta colección, se pudo comprobar de manera fiable que ambos términos se traducían como «seguridad tecnológica» y «seguridad física», respectivamente. Por otra parte, desde un punto de vista temático, se descubrió que, si bien las guías *Security of Radioactive Sources* y *Security in the Transport of Radioactive Material* abordaban la seguridad de las fuentes radiactivas para evitar su robo, sabotaje, acceso no autorizado, transferencia ilegal u usos dolosos, ambas tenían alcances diferentes. Esto confirmó cuán exhaustivo es el sistema de publicaciones del OIEA en cuanto al desarrollo de contenidos para los diferentes contextos en los que puede estar involucrado el material radiactivo. Finalmente, esta guía sobre transporte aparecía citada en la guía *Security of Radioactive Sources*, por lo que también ayuda a resolver necesidades informativas referenciales al brindar la versión oficial del nombre en español.

Como dato adicional, la versión traducida de esta guía presentó el mismo problema que las *Recomendaciones de seguridad física nuclear sobre materiales radiactivos e instalaciones conexa* en el menú de marcadores. En ambos casos, el menú de marcadores de contenidos era

funcional en la versión original en inglés, no así en la versión en español. En esta versión, el único marcador existente era uno titulado «_GoBack», que del todo no funcionaba.

3.4.5. *Computer Security at Nuclear Facilities*

Como parte de «Technical Guidance», se analizará la publicación titulada *Computer Security at Nuclear Facilities*, publicada en el 2011 (ver ficha descriptiva en el anexo 17). Su título en español es *Seguridad informática en las instalaciones nucleares*, versión que se publicó en el 2013 (ver ficha descriptiva en el anexo 18). Este documento contiene orientaciones y soluciones centradas en conservar la seguridad informática en las instalaciones nucleares. Para ello, se «recogen y describen las disposiciones especiales, las mejores prácticas y las enseñanzas extraídas aplicables a la disciplina nuclear (1). El contenido se divide en dos partes, una que sirve de guía para definir aspectos de gestión y otra que brinda orientaciones para la aplicación de las medidas de seguridad informática. Por tanto, las respuestas que pueda brindar esta publicación en relación con las necesidades terminológicas y temáticas planteadas para este trabajo son realmente limitadas. Su enfoque es la ciberseguridad aplicada a la protección de las fuentes radiactivas, por lo que su utilidad como fuente documental para la traducción de la guía *Security of Radioactive Sources* es muy limitada.

Puesto que esta publicación tiene un alcance muy específico dentro del campo de la protección del material radiactivo, se consideró que en aspectos de terminología y área de conocimiento es la que más se aleja de la guía *Security of Radioactive Sources*. Esto se puede ver más claro si se compara con las publicaciones analizadas anteriormente en este apartado. Además, este texto tampoco está citado en la guía que se está traduciendo, por lo que no resuelve una necesidad referencial específica. La guía *Seguridad informática en las instalaciones*

nucleares destaca como el único documento analizado de esta colección que no ayuda a solventar las necesidades informativas planteadas para este trabajo.

3.5. Conclusión

Las técnicas de búsquedas de recursos documentales que se emplearon en este capítulo sirvieron como base para obtener un banco de fuentes documentales que sirven no solo para la traducción de la guía *Security of Radioactive Sources*, sino para futuros trabajos relacionados con los documentos del OIEA y la seguridad de fuentes radiactivas en general. Se concluyó que cada una de las etapas de búsqueda podía tener una influencia positiva en las etapas posteriores, dado que ciertos elementos de evaluación que habían sido comentados anteriormente aplicaban a búsquedas posteriores. Además, gracias a ellas, era posible definir una estrategia más eficaz de obtener resultados que fueran de utilidad para la traducción. Por ejemplo, haber conocido el sistema de publicaciones del OIEA, al inicio de la investigación, llevó a que en la fase de búsqueda de textos paralelos no se requiriera del uso de un motor de búsqueda, sino que se utilizara directamente la página de la Colección de Seguridad Nuclear del OIEA. Esta fase de búsqueda de fuentes documentales ayuda a ir descartando recursos documentales que no son útiles y ahorrar tiempo en traducciones futuras. Por otra parte, se reconoció que un solo método de búsqueda puede no ser útil para todas las etapas, como sucedió con los términos de búsqueda que se utilizaron en la búsqueda de diccionarios o glosarios monolingües y bilingües. Esto resalta las características de flexibilidad, adaptabilidad e incluso improvisación que debería mostrar un traductor por la naturaleza de su trabajo. Las estrategias empleadas en este trabajo pueden aplicarse a la traducción de guías de seguridad física de fuentes radiactivas; no obstante, se reconoce que las mismas podrían ser útiles también en la traducción de otros tipos de textos que traten temas relacionados con fuentes radiactivas o el OIEA.

Conclusiones

La aplicación de estrategias de documentación en la traducción de la guía *Security of Radioactive Sources* permitió cumplir con los objetivos de esta investigación. A pesar de no contar con teoría que abordara específicamente el uso de técnicas documentales en la traducción de textos relacionados con fuentes radiactivas, fue posible proponer estrategias de documentación útiles en la traducción de la guía en estudio. Familiarizarse con el contexto dentro del cual se enmarcaba la guía e identificar las necesidades informativas del texto a traducir sentó las bases para la aplicación de estrategias de documentación que ayudaran a solventar los problemas traslativos. Sin embargo, se reconoce que por asuntos de enfoque y extensión de este trabajo, hubo estrategias documentales que no se pudieron explorar, tales como el uso de bases de datos terminológicas o la consulta a especialistas.

Las estrategias de documentación mostraron que, en ocasiones, las distintas necesidades informativas podrían solaparse, como fue el caso de *should*. Originalmente, esta palabra se analizó como una necesidad informativa terminológica del texto. Sin embargo, la fase de búsquedas de textos sobre la materia permitió encontrar las publicaciones *Categorization of Radioactive Sources* y su versión en español, *Clasificación de las fuentes radiactivas*, las cuales revelaron que el uso de este modal respondía al tipo de publicación; en ellas se explica que las guías emplean el modal *should* debido a que sus contenidos no tienen efectos vinculantes, en contraposición con los reglamentos, que emplean el modal *shall* porque sí son vinculantes (s. pag.). Este hallazgo reveló detalles sobre el tipo de publicaciones que contiene la Colección de Seguridad Física Nuclear del OIEA, dentro de la cual se encontraba la guía en estudio, lo que

hizo identificar el uso de *should* como una necesidad informativa temática, sin necesariamente dejar de ser terminológica.

En las fases iniciales de este estudio, se planteó como objetivo proponer un método de documentación que fuera aplicable a la traducción. Tal tarea suponía ofrecer los pasos a seguir, basados en estrategias documentales, a fin de garantizar una mejor traducción de la guía en estudio. Sin embargo, como se puede observar en este trabajo, las estrategias documentales que se aplicaron debieron ser variadas y, en más de una ocasión, adaptarse a cada necesidad informativa. Por esta razón, se consideró que lo más adecuado y provechoso sería ofrecer diferentes técnicas que pudieran ayudar a los traductores de guías de seguridad radiactiva a resolver problemas traductivos sin someterse a un proceso predeterminado traductológicos. Al pasar de métodos a estrategias, se brinda más flexibilidad al traductor para adaptar las estrategias a sus necesidades particulares. Un ejemplo de esto sucedió se ve ilustrado en el proceso de búsquedas que se llevó a cabo, donde, si bien se optó por emplear diferentes estrategias recomendadas por expertos en documentación aplicada a la traducción, las mismas debieron adaptarse a cada necesidad o modificarse con base en los resultados obtenidos. Se concluye que ofrecer estrategias documentales desarrolla las capacidades de adaptabilidad, toma de decisiones e incluso improvisación que debería saber utilizar un traductor para desarrollar su competencia en términos de alfabetización informacional.

Las estrategias empleadas en este trabajo también permitieron encontrar recursos documentales útiles dentro de los resultados encontrados en las fases de búsqueda. Un ejemplo de esto fue el hallazgo de un glosario monolingüe en inglés sobre fuentes radiactivas, creado por el OIEA y que se encontraba en fase de borrador a la fecha de realizar esta investigación en setiembre de 2016. Este glosario más actualizado se encontró dentro de la página del OIEA que

contenía el glosario monolingüe en inglés, oficial y vigente, el cual fue publicado en el 2007. Para no sobrepasar los alcances de esta investigación, este y otros resultados adicionales no fueron analizados. Sin embargo, en un trabajo de traducción, aplicar estas técnicas permitiría identificar y registrar debidamente recursos bibliográficos para futuros trabajos de traducción y, de esta manera, fortalecer el proceso de documentación y expeditar el proceso de investigación que conlleva la traducción

Otro resultado que se deriva de esta investigación fue la información de contacto de expertos en la materia o, en su defecto, formularios para realizar las consultas directamente a los especialistas, una de las etapas sugeridas por Merlo Vega. Si bien la búsqueda de especialistas sobrepasa el alcance de este proyecto, se reconoce que esta fase podría ser de gran ayuda para consultar información sobre terminología o temas desarrollados en el texto por traducir y posibles equivalentes en el idioma meta. Este paso también ayudaría a garantizar que los contenidos del texto traducido sean plenamente funcionales para los lectores meta, ya que se podría dar prioridad al uso del lenguaje técnico empleado por los mismos especialistas.

Esta investigación también permitió establecer que las etapas iniciales de documentación sientan las bases para las posteriores. Conocer el contexto dentro del cual se enmarcaba la guía *Security of Radioactive Sources* permitió descubrir el sistema de publicaciones del OIEA. A raíz de esto es que en la etapa de búsqueda de textos paralelos no se consideró necesario emplear Google, pues ya se contaba con un banco de publicaciones que se podía utilizar como base para tomar decisiones acerca de la forma de presentar la información en el texto traducido. Además, algunos resultados se repitieron en las diferentes búsquedas, por lo que, ya habiendo registrado una fuente documental, de repetirse en búsquedas posteriores, se podía pasar a revisar y registrar

otros textos que pudieran ser útiles. Este descubrimiento reveló que las diferentes etapas dan coherencia al proceso general de documentación que se lleva a cabo en la labor de la traducción.

Si bien este estudio se enfocó en la traducción de un texto técnico relacionado con la protección de fuentes radiactivas, abre toda una gama de temas de investigación. Como se comentó en la introducción de este trabajo, existe un vacío sobre estudios que aborden el uso de la documentación aplicada en la traducción de textos técnicos; para esta investigación, solo se encontró un estudio que trataba el uso de técnicas documentales aplicadas a la traducción de un texto relacionado con la vitivinicultura. Puesto que la bibliografía que se encontró para este trabajo abordaba la relación entre la documentación y la traducción desde una perspectiva muy general, en esta investigación se tuvo que indagar sobre diferentes estrategias documentales que fueran aplicables a la traducción de una guía sobre protección de fuentes radiactivas. Si se contara con estudios en diferentes campos, se podrían adaptar y proponer diferentes técnicas para nuevas áreas temáticas que puedan optimizar los procesos de traducción mediante la documentación. Por ejemplo, la fase de búsquedas podría variar con base en el documento que se deba traducir y los recursos a los que se tenga acceso, por lo que futuros investigadores podrían analizar los criterios bajo los cuales se deberían tomar tales decisiones. Y, más allá de los textos técnicos, también resultaría interesante aplicar las estrategias aquí desarrolladas en la traducción de textos literarios para descubrir de qué manera se deberían adaptar o cambiar estas estrategias. Esto podría revelar si los procesos de documentación aplicados a la traducción de textos literarios varían de suficiente manera como para abrir una nueva ventana de oportunidades en cuanto a estudios de documentación aplicada a la traducción.

Para el tema de traductores como usuarios de las estrategias documentales, se considera relevante realizar más investigaciones sobre las necesidades en cuanto a técnicas de

documentación y la capacidad de los recursos documentales existentes de cubrirlas. Por ejemplo, para este trabajo se encontraron diferentes artículos que proponían el uso de diferentes bases de datos y sistemas de documentación creados por entidades públicas y privadas para diferentes áreas temáticas; sin embargo, estos recursos se tuvieron que dejar de lado en este estudio porque no se adaptaban a las necesidades de la traducción de la guía *Security of Radioactive Sources* puesto que ninguno de los que se proponían se relacionaba con el tema de las fuentes radiactivas. Puesto que en muchas ocasiones la presión y los encargos a corto plazo obligan a limitar el tiempo dedicado a la investigación, sería de gran utilidad recolectar más conocimiento de estos recursos y hacer uso de técnicas de documentación que ayuden a agilizar el proceso y fortalecer las capacidades de traducción de los profesionales en este campo.

Bibliografía

Association of College and Research Libraries. «Presidential Committee on Information Literacy: Final Report». *American Library Association,* 1989. En línea. 24 jul. 2016.

Budinski, Kenneth G. «What is technical writing?». *Engineers' Guide to Technical Writing*. Ohio: ASM International, 2001. 1-16. Archivo PDF.

Byrne. Jody. «Scientific and Technical Translation». *Scientific and Technical Translation Explained*. Nueva York: Routledge, 2012. 1-24. Archivo PDF.

Chaves Barquero, Ana Lucía. «Atomic Spectrometry: AAnalyst 800 Atomic Absorption Spectrometer User's Guide: Influencia del lector meta en el proceso traductológico de textos técnicos». Trabajo de graduación. Universidad Nacional de Costa Rica, 2013. Archivo PDF.

Cid, Pilar y Remei Perpinyá. «Competencia informacional en traducción: análisis de los hábitos de los estudiantes universitarios en la consulta y uso de fuentes de información». *BiD: textos universitaris de biblioteconomia i documentació* 34 (2015). Archivo PDF. 24 jul. 2016.

«first responders radioactivity dictionary site:.org». *Google,* s.a. En línea. 5 nov. 2016.

Foro de la Industria Nuclear Española. *Foro Nuclear,* s.a. En línea. 8 oct. 2016.

---. «El experto te cuenta». *Foro Nuclear,* s.a. En línea. 8 oct. 2016.

---. «Enviar consulta al experto». *Foro Nuclear,* s.a. En línea. 8 oct. 2016.

---. «¿Qué es una fuente radiactiva y para qué sirve?». *Foro Nuclear,* 2016. En línea. 8 oct. 2016.

---. «Sobre nosotros». *Foro Nuclear,* s.a. En línea. 8 oct. 2016.

«fuentes radiactivas site:.org». *Google,* s.a. En línea. 5 nov. 2016.

«fuentes radiactivas en Costa Rica site:.go.cr»». *Google*, s.a. En línea. 5 nov. 2016.

«glosario oiea»». *Google*, s.a. En línea. 5 nov. 2016.

Gonzalo García, Consuelo y Esther Fraile Vicente. «Selección y evaluación de recursos lingüísticos en internet para el traductor especializado». *Manual de documentación y terminología para la traducción especializada*. Eds. Consuelo Gonzalo García y Valentín García Yebra. Madrid: Arco/Libros, 2004. 337-360. Impreso.

Ibáñez Rodríguez, Miguel. «La documentación en traducción especializada: el caso de la vitivinicultura». *El texto como encrucijada: estudios franceses y francófonos*. Madrid: Universidad de La Rioja, 2003. 537-551. Archivo PDF.

Merlo Vega, José Antonio. «Documentación aplicada a la traducción». *OpenCourseWare de la Universidad de Salamanca.* Salamanca: 2011, s. pag. Archivo PDF.

---. «Uso de la documentación en el proceso de traducción especializada». *Manual de documentación y terminología para la traducción especializada*. Eds. Consuelo Gonzalo García y Valentín García Yebra. Madrid: Arco/Libros, 2004. 309-374. Impreso.

Merlo Vega, José Antonio y Sonia Arroyo Izquierdo. «Documentación y traducción: Ámbitos de convergencia de dos disciplinas transversales». *Puntos de encuentro: Los primeros 20 años de la facultad de traducción y documentación de la Universidad de Salamanca*. Salamanca: Ediciones Universidad de Salamanca, 2013. 119-131. Archivo PDF.

Ministerio de Salud de Costa Rica. *Decreto No. 24037-S: Reglamento sobre protección contra las radiaciones ionizantes*. Costa Rica: La Gaceta, 1995. Archivo PDF.

---. «Decreto No. 24037-S: Reglamento sobre protección contra las radiaciones ionizantes». *Sistema Costarricense de Información Jurídica*, 2009. En línea. 10 de noviembre de 2016.

Organismo Internacional de Energía Atómica. «Clasificación de las fuentes radiactivas». *IAEA*, s.a. En línea. 24 de octubre de 2016.

---. *Code of Conduct on the Safety and Security of Radioactive Sources*. Austria: IAEA, 2004. PDF.

---. *Computer Security at Nuclear Facilities*. Viena: IAEA, 2011. Archivo PDF.

---. *Colección Seguridad No. 115*. Viena: IAEA, 1997. Archivo PDF.

---. «Forthcoming IAEA Nuclear Security Series Publications». *IAEA*. En línea. 4 de setiembre 2016.

---. *Glosario de seguridad tecnológica del OIEA*. Viena: IAEA, 2007. Archivo PDF.

---. *Clasificación de las fuentes radiactivas*. Viena: IAEA, 2009. Archivo PDF.

---. «IAEA Safety Glossary». *IAEA*, s.a. En línea. 8 de octubre de 2016.

---. *IAEA Safety Glossary*. Viena: IAEA, 2007. Archivo PDF.

---. *IAEA Safety Glossary: 2016 Revision*. Viena: IAEA, 2016. Archivo PDF.

---. *La seguridad física en el transporte de materiales radiactivos*. Viena: IAEA, 2013. Archivo PDF.

---. «Member States». IAEA. En línea. 20 mayo 2016.

---. *Normas básicas internacionales de seguridad para la protección contra la radiación ionizante y para la seguridad de las fuentes de radiación*. Viena: IAEA, 1997. Archivo PDF.

---. «Normas básicas internacionales de seguridad para la protección contra la radiación ionizante y para la seguridad de las fuentes de radiación». *Organización Internacional del Trabajo*, s.a. En línea. 24 de octubre de 2016.

---. *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*. Viena: IAEA, 2011. Archivo PDF.

---. «Nuclear Security Series». *IAEA*. En línea. 4 de setiembre 2016.

---. «Nuclear Security Series Publications». *IAEA*, s.a. En línea. 12 de setiembre de 2016.

---. *Objective and Essential Elements of a State's Nuclear Security Regime*. Viena: IAEA, 2013. Archivo PDF.

---. *Objetivo y elementos esenciales del régimen de seguridad física nuclear de un Estado*. Viena: IAEA, 2014. Archivo PDF.

---. *Recomendaciones de seguridad física nuclear sobre la protección física de los materiales y las instalaciones nucleares*. Viena: IAEA, 2012. Archivo PDF.

---. *Recomendaciones de Seguridad Física Nuclear sobre Materiales Radiactivos e Instalaciones Conexas*. Viena: IAEA, 2012. Archivo PDF.

---. «Review Committees». *IAEA*. En línea. 4 de setiembre 2016.

---. «Scientific and Technical Publications». *IAEA*. En línea. 4 de setiembre 2016.

---. «Secretariat». IAEA. En línea. 20 mayo 2016.

---. *Security in the Transport of Radioactive Material*. Viena: IAEA, 2008. Archivo PDF.

---. *Security of Radioactive Sources*. Viena: IAEA, 2009. Archivo PDF.

---. *Seguridad informática en las instalaciones nucleares*. Viena: IAEA, 2013. Archivo PDF.

Ortoll Espinet, Eva. «Competencia informacional para la actividad traductora». *Tradumàtica*, vol. 2 (2003). Archivo PDF.

Pinto, María. Calidad y evaluación de los contenidos electrónicos. «Electronic Content Management Skills». *Mariapinto.es*. S. f. En línea. 14 ag. 2016.

Radiation Emergency Medical Management. «About This Site». *Radiation Emergency Medical Management*, 2016. En línea. 28 oct. 2016.

---. «Dictionary of Radiation Terms». *Radiation Emergency Medical Management*, 2016. En línea. 28 oct. 2016.

Recoder, María José y Pilar Cid. «La documentación en la traducción especializada». Eds. Gonzalo García, Consuelo y Valentín García Yebra. *Manual de documentación y terminología para la traducción especializada*. Madrid: Arco/Libros, 2004. 73-88. Impreso.

---. «Traducción y documentación: cooperar para difundir la información». *Hipertext* 1 (2003): s. pag. En línea. 24 jul. 2016.

Anexos

Anexo 1: Ficha Modelo

Datos del documento o página web		
Nombre del archivo o página web		
Dirección URL de visita o descarga		
Fecha de consulta		
Idioma		
Breve descripción del contenido		
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido		☐
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización		☐
Gramática y vocabulario aceptables		☐
Afinidad con el TO		☐
Compatibilidad		
Formato funcional		☐
Versiones en otras lenguas		☐
Funcionalidad y navegabilidad		
Estructura y organización lógicas		☐
Menú/marcadores de contenido funcionales		☐
Diseño		
Diseño funcional		☐
Adecuada combinación de colores y formas		☐
Tipografía adecuada		☐
Pertinencia		
Necesidades informativas terminológicas ☐	Necesidades informativas temáticas ☐	Necesidades informativas referenciales ☐

Anexo 2

Datos del documento o página web		
Nombre del archivo o página web	*Dictionary of Radiation Terms de la REMM*	
Dirección URL de visita o descarga	https://www.remm.nlm.gov/dictionary.htm	
Fecha de consulta	28 de octubre	
Idioma	Inglés	
Breve descripción del contenido	Diccionario en inglés con definiciones de palabras y enlaces relacionados con el uso de la radiación dentro del campo médico. Dentro de las definiciones se encuentran enlaces que llevan a otras páginas web (dentro del sitio de la REMM o externas) donde se definen términos más a profundidad.	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	Department of Health and Human Services, Office of the Assistant Secretary for Preparedness and Response, Office of Planning and Emergency Operations, National Library of Medicine, Division of Specialized Information Services, expertos en la materia del National Cancer Institute, Centers for Disease Control and Prevention, y asesores externos.	☒
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	Última actualización el 16 de agosto de 2016	☒
Gramática y vocabulario aceptables		☒
Afinidad con el TO	Se relaciona más con el campo médico que con la seguridad de fuentes radiactivas.	☐
Compatibilidad		
Formato funcional	HTML	☒
Versiones en otras lenguas		☐
Funcionalidad y navegabilidad		
Estructura y organización lógicas		☐
Menú/marcadores de contenido funcionales	No tiene.	☐
Diseño		
Diseño funcional	Hizo falta menú de contenidos	☐
Adecuada combinación de colores y formas		☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☒	Necesidades informativas temáticas ☐	Necesidades informativas referenciales ☐

Anexo 3

Datos del documento o página web		
Nombre del archivo o página web	*IAEA Safety Glossary*	
Dirección URL de visita o descarga	http://www-ns.iaea.org/downloads/standards/glossary/glossary-english-version2point0-sept-06-12.pdf	
Fecha de consulta	28/10/16	
Idioma	Inglés	
Breve descripción del contenido	Glosario monolingüe de seguridad radiológica creado por el OIEA para armonizar el uso de la terminología dentro del organismo. Los términos son definidos y se añaden, de ser necesario, aclaraciones o referencias a otros términos dentro del mismo glosario.	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	OIEA	☒
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	2006	☒
Gramática y vocabulario aceptables		☒
Afinidad con el TO		☒
Compatibilidad		
Formato funcional	PDF	☒
Versiones en otras lenguas	Árabe, chino, español francés y ruso	☒
Funcionalidad y navegabilidad		
Estructura y organización lógicas	Orden alfabético y referencias a otros términos dentro del glosario	☒
Menú/marcadores de contenido funcionales		☒
Diseño		
Diseño funcional	Sí, aunque el menú pudo haberse mejorado	☒
Adecuada combinación de colores y formas		☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☒	Necesidades informativas temáticas ☐	Necesidades informativas referenciales ☒

Anexo 4

Datos del documento o página web		
Nombre del archivo o página web	*Glosario de seguridad tecnológica del OIEA*	
Dirección URL de visita o descarga	http://www-pub.iaea.org/MTCD/publications/PDF/IAEASafetyGlossary2007/Glossary/SafetyGlossary_2007s.pdf	
Fecha de consulta	8 de octubre de 2016	
Idioma	Español	
Breve descripción del contenido	Glosario de términos relacionados con la seguridad nuclear y la protección contra la radiación. Además de la definición en español, incluye el equivalente en inglés.	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	OIEA (IAEA)	☒
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	2007	☒
Gramática y vocabulario aceptables		☐
Afinidad con el TO		☐
Compatibilidad		
Formato funcional	PDF	☒
Versiones en otras lenguas	Árabe, chino, francés, inglés y ruso	☒
Funcionalidad y navegabilidad		
Estructura y organización lógicas	Orden alfabético adecuado	☐
Menú/marcadores de contenido funcionales		☐
Diseño		
Diseño funcional	Funcional, no necesariamente atractivo	☐
Adecuada combinación de colores y formas	Muy formal	☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☒	Necesidades informativas temáticas ☐	Necesidades informativas referenciales ☒

Anexo 5

Datos del documento o página web		
Nombre del archivo o página web	*Glosario de la Colección Seguridad No. 115*	
Dirección URL de visita o descarga	**Glosario**: http://www-pub.iaea.org/MTCD/publications/PDF/SS-115s-Web/Pub996s6.pdf **Colección Seguridad No. 115**: http://www.ilo.org/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/publication/wcms_154389.pdf	
Fecha de consulta	1996	
Idioma	Español	
Breve descripción del contenido	Normas internacionales relacionadas con los requisitos de seguridad y protección de las fuentes radiactivas en la medicina y el comercio. Dentro de esta colección, se incluye un glosario relacionado con los mismos temas.	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	OIEA	☐
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	1997	☐
Gramática y vocabulario aceptables		☒
Afinidad con el TO		☒
Compatibilidad		
Formato funcional	PDF	☒
Versiones en otras lenguas	Árabe, chino, francés, inglés y ruso	☒
Funcionalidad y navegabilidad		
Estructura y organización lógicas		☒
Menú/marcadores de contenido funcionales	A la izquierda.	☒
Diseño		
Diseño funcional	Parece ser escaneado. Lucen más nítidas las publicaciones más recientes.	☒
Adecuada combinación de colores y formas	Formal.	☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☒	Necesidades informativas temáticas ☒	Necesidades informativas referenciales ☒

Anexo 6

Datos del documento o página web		
Nombre del archivo o página web	*Clasificación de las fuentes radiactivas*	
Dirección URL de visita o descarga	http://www-pub.iaea.org/MTCD/publications/PDF/Pub1227s_web.pdf	
Fecha de consulta	8 de octubre de 2016	
Idioma	Español	
Breve descripción del contenido	Información detallada sobre la clasificación de las fuentes radiactivas con base en el riesgo, las fuentes y las prácticas. Además, sirve de guía para clasificar las fuentes. Cuenta con varios cuadros.	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	OIEA	☒
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	2009	☒
Gramática y vocabulario aceptables		☒
Afinidad con el TO		☒
Compatibilidad		
Formato funcional	PDF	☒
Versiones en otras lenguas	Árabe, chino, inglés, francés y ruso	☒
Funcionalidad y navegabilidad		
Estructura y organización lógicas		☒
Menú/marcadores de contenido funcionales	Al lado izquierdo	☒
Diseño		
Diseño funcional		☒
Adecuada combinación de colores y formas	Formal	☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☒	Necesidades informativas temáticas ☒	Necesidades informativas referenciales ☒

Anexo 7

Datos del documento o página web		
Nombre del archivo o página web	«¿Qué es una fuente radiactiva y para qué sirve?»	
Dirección URL de visita o descarga	http://www.foronuclear.org/en/el-experto-te-cuenta/120957-ique-es-una-fuente-radiactiva-y-para-que-sirve	
Fecha de consulta	8 de octubre de 2016	
Idioma	Español	
Breve descripción del contenido	Pocos párrafos en los que se brinda información general sobre las fuentes radiactivas (uso, control, registro, fuentes huérfanas). En los enlaces de la misma página se puede encontrar más información sobre diferentes temas relacionados con el uso de la energía nuclear; los contenidos son explicados de manera sencilla.	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	2014. El resto de enlaces tienen fechas de actualización variadas pero recientes.	☒
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	2014. El resto de enlaces tienen fechas de actualización variadas pero recientes.	☒
Gramática y vocabulario aceptables		☒
Afinidad con el TO		☒
Compatibilidad		
Formato funcional	HTML	☐
Versiones en otras lenguas	Inglés	☐
Funcionalidad y navegabilidad		
Estructura y organización lógicas	Tres subtítulos y enlaces de fácil acceso	☐
Menú/marcadores de contenido funcionales	Al lado izquierdo se encuentran dos enlaces, «Consultas al experto» y «El experto te cuenta», que llevan a otros enlaces relacionados con la energía nuclear.	☐
Diseño		
Diseño funcional	El diseño se consideró adecuado.	☒
Adecuada combinación de colores y formas		☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☐	Necesidades informativas temáticas ☒	Necesidades informativas referenciales ☐

Anexo 8

Datos del documento o página web		
Nombre del archivo o página web	«Autorizaciones y certificaciones del Ministerio de Salud»	
Dirección URL de visita o descarga	http://www.ministeriodesalud.go.cr/index.php/tramites-ms/autorizaciones-y-certificados?id=656	
Fecha de consulta	10 de noviembre de 2016	
Idioma	Español	
Breve descripción del contenido	Enlaces a leyes, formularios y guías para la elaboración de certificados y manuales de procedimientos relacionados con material radiactivo	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	Ministerio de Salud de Costa Rica	☒
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	Cada autorización y certificación tiene fechas de emisión diferentes	☐
Gramática y vocabulario aceptables		☒
Afinidad con el TO	Los enlaces sí, pero no el contenido de la página per se	☐
Compatibilidad		
Formato funcional	HTML	☒
Versiones en otras lenguas		☐
Funcionalidad y navegabilidad		
Estructura y organización lógicas	Existe una clasificación de los documentos que se puede descargar.	☒
Menú/marcadores de contenido funcionales	Visible y funcional.	☒
Diseño		
Diseño funcional		☒
Adecuada combinación de colores y formas		☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☐	Necesidades informativas temáticas ☒	Necesidades informativas referenciales ☐

Anexo 9

Datos del documento o página web		
Nombre del archivo o página web	*Decreto No. 24037-S: Reglamento sobre protección contra las radiaciones ionizantes*	
Dirección URL de visita o descarga	http://www.cea.go.cr/publicaciones/Reglamento_proteccion_radiologica.pdf	
Fecha de consulta	1 de noviembre de 2016	
Idioma	Español	
Breve descripción del contenido	Reglamento para todo lo relacionado con la protección contra la radiación, por ejemplo, la autoridad reguladora, las instalaciones, los operadores, el transporte, importación, exportación, inspecciones, desecho, dosimetría, emergencias radiológicas, etc.	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	Ministerio de Salud de Costa Rica	☐
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	Publicado el 8 de marzo de 1995. Se debería buscar un reglamento más reciente.	☐
Gramática y vocabulario aceptables		☒
Afinidad con el TO	Refleja el uso que se le podría dar a la guía.	☒
Compatibilidad		
Formato funcional	PDF	☒
Versiones en otras lenguas		☐
Funcionalidad y navegabilidad		
Estructura y organización lógicas	Normal de un reglamento.	☒
Menú/marcadores de contenido funcionales		☐
Diseño		
Diseño funcional	Formal.	☒
Adecuada combinación de colores y formas		☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☐	Necesidades informativas temáticas ☒	Necesidades informativas referenciales ☐

Anexo 10

Datos del documento o página web		
Nombre del archivo o página web	«Ministerio de Salud informa sobre robo de equipo con fuente radiactiva»	
Dirección URL de visita o descarga	http://www.ministeriodesalud.go.cr/index.php/centro-de-prensa/noticias/727-noticias-2016/873-ministerio-de-salud-informa-sobre-robo-de-equipo-con-fuente-radiactiva	
Fecha de consulta	10 de noviembre de 2016	
Idioma	Español	
Breve descripción del contenido	Comunicado de prensa donde se informa sobre el robo de un densímetro nuclear y se pide ayuda a la población para obtener información al respecto	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	Oficina de prensa del Ministerio de Salud	☒
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	Publicado el 8 de marzo del 2016	☒
Gramática y vocabulario aceptables		☒
Afinidad con el TO	Muestra el peligro al que se exponen las fuentes y los riesgos que representan.	☒
Compatibilidad		
Formato funcional	HTML	☒
Versiones en otras lenguas		☐
Funcionalidad y navegabilidad		
Estructura y organización lógicas	Es un comunicado corto y conciso.	☒
Menú/marcadores de contenido funcionales	A otros comunicados.	☒
Diseño		
Diseño funcional		☒
Adecuada combinación de colores y formas		☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☐	Necesidades informativas temáticas ☒	Necesidades informativas referenciales ☐

Anexo 11

Datos del documento o página web		
Nombre del archivo o página web	*Objective and Essential Elements of a State's Nuclear Security Regime*	
Dirección URL de visita o descarga	http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf	
Fecha de consulta	8 de octubre de 2016	
Idioma	Inglés	
Breve descripción del contenido	Nociones Fundamentales de Seguridad Física Nuclear. Esta publicación buscar ayudar a los Estados en la creación de un marco legal sólido en materia de seguridad nuclear. Incluye los objetivos que se deben cumplir y los elementos fundamentales a incluir. Publicación pequeña.	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	OIEA	☒
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	2013	☒
Gramática y vocabulario aceptables		☒
Afinidad con el TO	Pertenece a la Colección de Seguridad Física Nuclear del OIEA.	☒
Compatibilidad		
Formato funcional	PDF	☒
Versiones en otras lenguas	Árabe, chino, francés, ruso y español	☒
Funcionalidad y navegabilidad		
Estructura y organización lógicas	Adecuados.	☒
Menú/marcadores de contenido funcionales	Presente y funcional.	☒
Diseño		
Diseño funcional		☒
Adecuada combinación de colores y formas		☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☒	Necesidades informativas temáticas ☒	Necesidades informativas referenciales ☐

Anexo 12

Datos del documento o página web		
Nombre del archivo o página web	*Objetivo y elementos esenciales del régimen de seguridad física nuclear de un Estado*	
Dirección URL de visita o descarga	http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590s_web.pdf	
Fecha de consulta	8 de octubre de 2016	
Idioma	Español	
Breve descripción del contenido	Nociones Fundamentales de Seguridad Física Nuclear. Esta publicación buscar ayudar a los Estados en la creación de un marco legal sólido en materia de seguridad nuclear. Incluye los objetivos que se deben cumplir y los elementos fundamentales a incluir.	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido		☒
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	2014	☒
Gramática y vocabulario aceptables		☒
Afinidad con el TO	Pertenece a la Colección de Seguridad Física Nuclear del OIEA.	☒
Compatibilidad		
Formato funcional	PDF	☒
Versiones en otras lenguas	Árabe, chino, francés, inglés y ruso	☒
Funcionalidad y navegabilidad		
Estructura y organización lógicas	Adecuados.	☒
Menú/marcadores de contenido funcionales	Los dos marcadores no son funcionales y parecen más bien errores.	☐
Diseño		
Diseño funcional		☒
Adecuada combinación de colores y formas		☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☒	Necesidades informativas temáticas ☒	Necesidades informativas referenciales ☐

Anexo 13

Datos del documento o página web		
Nombre del archivo o página web	*Nuclear Security Recommendations on Radioactive Material and Associated Facilities*	
Dirección URL de visita o descarga	http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1487_web.pdf	
Fecha de consulta	8 de octubre de 2016	
Idioma	Inglés	
Breve descripción del contenido	Recomendaciones. Esta publicación ofrece recomendaciones sobre cómo crear un marco reglamentario en materia nuclear para la protección del material radiactivo, y las instalaciones y actividades relacionadas.	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	OIEA	☒
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	2011	☒
Gramática y vocabulario aceptables		☒
Afinidad con el TO	Pertenece a la Colección de Seguridad Física Nuclear del OIEA y aparece citado en la guía.	☒
Compatibilidad		
Formato funcional	PDF	☒
Versiones en otras lenguas	Árabe, chino, francés, ruso y español.	☒
Funcionalidad y navegabilidad		
Estructura y organización lógicas	Adecuados.	☒
Menú/marcadores de contenido funcionales	Presente y funcional.	☒
Diseño		
Diseño funcional		☒
Adecuada combinación de colores y formas		☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☒	Necesidades informativas temáticas ☒	Necesidades informativas referenciales ☒

Anexo 14

Datos del documento o página web		
Nombre del archivo o página web	*Recomendaciones de seguridad física nuclear sobre materiales radiactivos e instalaciones conexas*	
Dirección URL de visita o descarga	http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1487s_web.pdf	
Fecha de consulta	8 de octubre de 2016	
Idioma	Español	
Breve descripción del contenido	Esta publicación ofrece recomendaciones sobre cómo crear un marco reglamentario en materia nuclear para la protección del material radiactivo, las instalaciones y actividades relacionadas.	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	OIEA	☒
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	2012	☒
Gramática y vocabulario aceptables		☒
Afinidad con el TO	Pertenece a la Colección de Seguridad Física Nuclear del OIEA y aparece citado en la guía.	☒
Compatibilidad		
Formato funcional	PDF	☒
Versiones en otras lenguas	Árabe, chino, francés, inglés y ruso.	☒
Funcionalidad y navegabilidad		
Estructura y organización lógicas	Adecuados.	☒
Menú/marcadores de contenido funcionales	Presente y funcional.	☒
Diseño		
Diseño funcional		☒
Adecuada combinación de colores y formas		☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☒	Necesidades informativas temáticas ☒	Necesidades informativas referenciales ☒

Anexo 15

Datos del documento o página web		
Nombre del archivo o página web	*Security in the Transport of Radioactive Material*	
Dirección URL de visita o descarga	http://www-pub.iaea.org/books/IAEABooks/7987/Security-in-the-Transport-of-Radioactive-Material http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1348_web.pdf	
Fecha de consulta	28 de octubre de 2016	
Idioma	Inglés	
Breve descripción del contenido	Guía de implementación de reglamentos que rijan la seguridad física de las fuentes radiactivas durante su transporte doméstico e internacional	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	OIEA	☒
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	2008	☒
Gramática y vocabulario aceptables		☒
Afinidad con el TO	Pertenece a la Colección de Seguridad Física Nuclear del OIEA y aparece citado en la guía.	☒
Compatibilidad		
Formato funcional	PDF	☒
Versiones en otras lenguas	Chino, francés y español	☒
Funcionalidad y navegabilidad		
Estructura y organización lógicas	Adecuados.	☒
Menú/marcadores de contenido funcionales	Presente y funcional.	☒
Diseño		
Diseño funcional		☒
Adecuada combinación de colores y formas		☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☒	Necesidades informativas temáticas ☒	Necesidades informativas referenciales ☒

Anexo 16

Datos del documento o página web		
Nombre del archivo o página web	*La seguridad física en el transporte de materiales radiactivos*	
Dirección URL de visita o descarga	http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1348s_web.pdf	
Fecha de consulta	28 de octubre de 2016	
Idioma	Español	
Breve descripción del contenido	Guía de implementación de reglamentos que rijan la seguridad física de las fuentes radiactivas durante su transporte doméstico e internacional	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	OIEA	☒
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	2013	☒
Gramática y vocabulario aceptables		☒
Afinidad con el TO	Pertenece a la Colección de Seguridad Física Nuclear del OIEA y aparece citado en la guía.	☒
Compatibilidad		
Formato funcional	PDF	☒
Versiones en otras lenguas	Chino, inglés y francés	☒
Funcionalidad y navegabilidad		
Estructura y organización lógicas	Adecuados.	☒
Menú/marcadores de contenido funcionales	Menú de marcadores de contenido no funcional. Sólo existe un marcador y es erróneo	☐
Diseño		
Diseño funcional		☒
Adecuada combinación de colores y formas		☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☒	Necesidades informativas temáticas ☒	Necesidades informativas referenciales ☒

Anexo 17

Datos del documento o página web		
Nombre del archivo o página web	*Computer Security at Nuclear Facilities*	
Dirección URL de visita o descarga	http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf	
Fecha de consulta	10 de noviembre de 2016	
Idioma	Inglés	
Breve descripción del contenido	Ofrece guía técnica sobre la seguridad informática aplicada a las instalaciones en las que se empleen fuentes radiactivas	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	OIEA	☒
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	2011	☒
Gramática y vocabulario aceptables		☒
Afinidad con el TO	Su única relación es pertenecer a la misma colección de seguridad, pero sus contenidos no se relacionan con la protección directa de las fuentes radiactivas.	☐
Compatibilidad		
Formato funcional	PDF	☒
Versiones en otras lenguas	Árabe, chino, francés, ruso y español	☒
Funcionalidad y navegabilidad		
Estructura y organización lógicas	Adecuados.	☒
Menú/marcadores de contenido funcionales	Presente y funcional.	☒
Diseño		
Diseño funcional		☒
Adecuada combinación de colores y formas		☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☐	Necesidades informativas temáticas ☐	Necesidades informativas referenciales ☐

Anexo 18

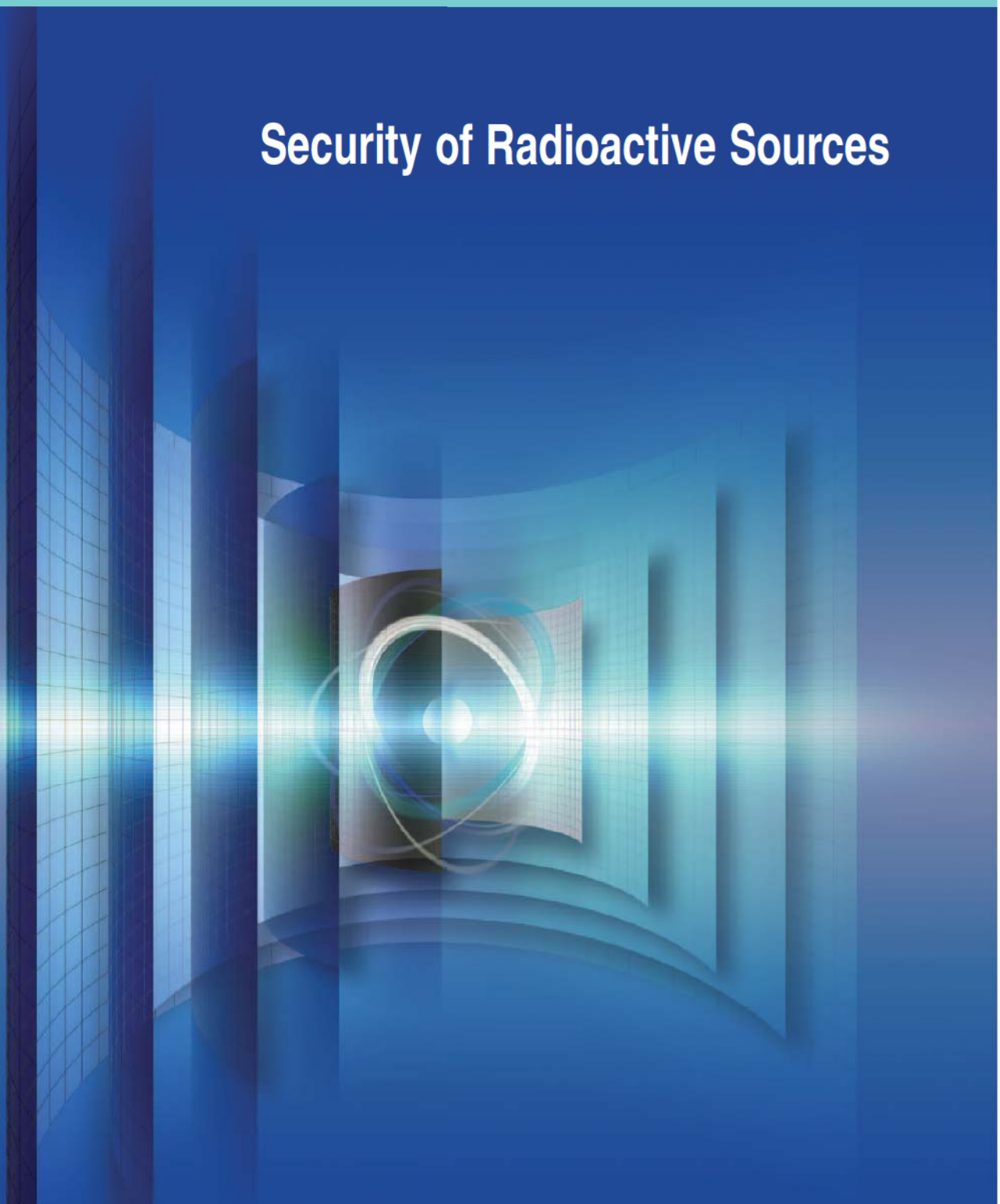
Datos del documento o página web		
Nombre del archivo o página web	Seguridad informática en las instalaciones nucleares	
Dirección URL de visita o descarga	http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527s_web.pdf	
Fecha de consulta	10 de noviembre de 2016	
Idioma	Español	
Breve descripción del contenido	Ofrece guía técnica sobre la seguridad informática aplicada a las instalaciones en las que se empleen fuentes radiactivas	
Criterios	**Parámetros y comentarios**	**Cumple con el criterio**
Autoría		
Autor reconocido	OIEA	☒
Contenido y uso del lenguaje		
Fecha reciente de creación y actualización	2013	☒
Gramática y vocabulario aceptables		☒
Afinidad con el TO	Su única relación es pertenecer a la misma colección de seguridad, pero sus contenidos no se relacionan con la protección directa de las fuentes radiactivas.	☐
Compatibilidad		
Formato funcional	PDF	☒
Versiones en otras lenguas	Árabe, chino, francés, inglés y ruso	☒
Funcionalidad y navegabilidad		
Estructura y organización lógicas		☒
Menú/marcadores de contenido funcionales	Inexistente.	☐
Diseño		
Diseño funcional		☒
Adecuada combinación de colores y formas		☒
Tipografía adecuada		☒
Pertinencia		
Necesidades informativas terminológicas ☐	Necesidades informativas temáticas ☐	Necesidades informativas referenciales ☐

El texto original

IAEA Nuclear Security Series No. 11

Implementing Guide

Security of Radioactive Sources



IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES No. 11

SECURITY OF RADIOACTIVE SOURCES

IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2009

1. INTRODUCTION

1.1. BACKGROUND

This publication offers guidance for implementing security measures on radioactive sources. It also provides advice on implementing security related provisions in the Code of Conduct on the Safety and Security of Radioactive Sources [1] (hereafter referred to as the 'Code of Conduct') (see the Definitions for explanations of the terms in this publication).

This Implementing Guide, while replacing Security of Radioactive Sources — Interim Guidance for Comment (IAEA-TECDOC-1355) [2], takes account of the overall security approach established in that publication which some States may have used as a reference in devising their current security regimes. This publication has been harmonized with the IAEA's Categorization of Radioactive Sources [3] and proposes a graded approach to security using a set of security levels, and the security functions of deterrence, detection, delay, response and security management.

This publication should be read in conjunction with the Code of Conduct [1], the Categorization of Radioactive Sources [3], the Safety of Radiation Generators and Sealed Radioactive Sources [4], the International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources [5], and the IAEA Fundamental Safety Principles [6].

Finally, this guide recognizes that there should be a balance between managing sources securely while still enabling them to be used safely by authorized personnel. Since radioactive sources are an integral and critical tool in the world's health care, manufacturing, research and quality control industries, care needs to be taken to ensure that the many beneficial uses of sources are not unduly hindered. The challenge for the regulatory body, users and other stakeholders is to find the correct point of balance.

1.2. OBJECTIVE

This publication is intended for use by States in formulating security policy for radioactive sources and by regulatory bodies in developing regulatory requirements that are consistent with the Code of Conduct. It will also assist State parties to fulfil certain obligations under the International Convention for the Suppression of Acts of Nuclear Terrorism [7]. It may also be useful to operators managing radioactive sources in developing their security programmes.

1.3. SCOPE

This publication includes guidance and recommended measures for the prevention of, detection of, and response to malicious acts involving radioactive sources. It will also help towards preventing the loss of control of such sources. It does not apply to nuclear material as defined in the Convention on the Physical Protection of Nuclear Material and the Amendment thereto [8], except for sources incorporating plutonium-239.

While this guide does not specifically address the security of unsealed radioactive material, a State may choose to apply the security concepts and measures outlined in this guide to such material.

This publication recommends that security measures be applied to radioactive sources in manufacture, use and short term or long term storage (see the Definitions).

This guide recommends that security measures be applied on a graded basis, taking into account the current evaluation of the threat, the relative attractiveness of the source, and the potential consequences resulting from malicious use. The requisite level of security is achieved through a combination of deterrence, detection, delay, response and security management.

States may decide that some or all sources are at greater or lesser risk than the basis on which this guide was written. In such cases States will need to have the flexibility to vary the security measures they require, compared with those that are recommended here. When doing this, States will need to remain within the overall structure of this guide as much as possible.

This guide does not include recommendations on emergency preparedness and response, intervention, or the remediation of contaminated areas. Such guidance is available in other IAEA publications [5, 9, 10]. Guidance on protecting people against radiation in the aftermath of an attack is given by the International Commission on Radiological Protection [11].

Finally, this publication does not deal with radioactive material, including radioactive sources, while in transport. Such guidance, including that for third party shippers, is given in Ref. [12].

2. RESPONSIBILITIES OF THE STATE AND OPERATOR

2.1. INTRODUCTION

The Code of Conduct [1] recognizes that an effective national system of regulatory control underpins the safety and security of radioactive sources in a State. This section provides further guidance on the responsibilities of the State and the operator with regard to the security of radioactive sources.

2.2. STATE

Every State will need to define its domestic threat (see Section 3.8.1). This process needs to begin with a national threat assessment, which is an analysis that documents — at a national level — the credible motivations, intentions and capabilities of potential adversaries that could cause harm through the sabotage of a facility or the unauthorized removal of a radioactive source for malicious purposes. Guidance on this topic is discussed in detail in Ref. [13].

Every State will need to take the appropriate measures to ensure that radioactive sources within its territory, or under its jurisdiction or control, are securely protected during and at the end of their useful lives. This includes the promotion of a security culture with regard to radioactive sources and adequate education and training of regulators and operators.

States will need to have an effective national legislative and regulatory infrastructure in place to govern the security of radioactive sources, which:

- Prescribes and assigns governmental responsibilities to relevant bodies including an independent regulatory body to establish, implement, and maintain a regime that ensures the security of radioactive sources;
- Establishes security requirements for radioactive sources and includes a system of evaluation, licensing, and enforcement or other procedures to grant authorizations;
- Places the prime responsibility for the security of radioactive sources on the operators;
- Provides for measures to reduce the likelihood of the attempt of malicious acts;
- Provides for measures that mitigate/minimize the consequences of malicious acts involving radioactive sources;

— Establishes punishable offences covering malicious acts involving radioactive sources;

The implementation and operation of the legislative and regulatory infrastructure for the security of radioactive sources rely on the effective cooperation between the various bodies assigned governmental responsibilities. Typically, these bodies are likely to include a State's regulatory body, intelligence community, ministries of interior, defence, transportation, and foreign affairs; law enforcement; customs and coast guard and other agencies with security related responsibilities.

States will need to ensure that the regulatory body is adequately resourced, in terms of personnel and funding, to fulfil its regulatory functions, including implementing an inspection programme to verify that the security of radioactive sources is effectively maintained. This inspection programme should be supported by written procedures and performed by qualified personnel. The frequency of inspections should take account of the security level (see Section 4.1) of the radioactive source(s) and may consider an operator's past performance in maintaining compliance with security requirements. Inspections of security measures implemented by an operator can be performed together with inspections for verifying compliance with other regulatory requirements, such as safety, or as stand-alone inspections.

2.3. OPERATORS

Operators, as the authorized entities, should have the primary responsibility for implementing and maintaining security measures for radioactive sources in accordance with national requirements. Operators may, depending on a State's regulatory requirements, appoint or contract a third party to carry out actions and tasks related to the security of radioactive sources, although the authorized operator should retain the prime responsibility for regulatory compliance and effectiveness of the actions and tasks. Also, operators should ensure that their personnel and their contractors are suitably trained and meet the regulatory requirements, which should include trustworthiness.

Operators should verify that sources are present at their authorized location at prescribed intervals. Any absence or discrepancy should be promptly investigated and reported to the regulatory body. Processes should be in place to ensure that all Category 1, 2, and 3 sources (see Section 4.2.1) for which operators are authorized are identifiable and traceable.

When required by the regulatory authorities, operators should carry out vulnerability assessments (see the Definitions) of their radioactive sources based on the current assessed threat.

Operators should promote a security culture (see Section 3.2), and establish a management system commensurate with the levels of security (see Section 4.1), to ensure that:

— Policies and procedures are established that identify security as being of high priority;
— Problems affecting security are promptly identified and corrected in a manner commensurate with their importance;
— The responsibilities of each individual for security are clearly identified and each individual is suitably trained, qualified, and determined to be trustworthy;
— Clear lines of authority for decisions on security are defined;
— Organizational arrangements and lines of communications are established that result in an appropriate flow of information on security within the entire organization;
— Sensitive information is identified and protected according to national regulations;
— Radioactive sources are managed in accordance with a security plan (see the Definitions), when required by the regulatory body.

3. SECURITY CONCEPTS

3.1. INTRODUCTION

This section introduces the basic principles applicable to the security of radioactive sources established in the Code of Conduct [1], and then elaborates on security concepts, including the basic security functions of deterrence, detection, delay, response and security management (Table 1).

3.2. SECURITY CULTURE

A dynamic and effective security culture should exist at all levels of operator staff and management.

TABLE 1. PRINCIPLES FROM THE CODE OF CONDUCT FOR THE SECURITY OF RADIOACTIVE SOURCES

The Code of Conduct establishes basic principles applicable to the security of radioactive sources, several of which are relevant to this publication. According to these principles, every State has:

- To take the appropriate measures necessary to ensure that radioactive sources are **"securely protected during their useful lives and at the end of their useful lives"** (paragraph 7);
- To emphasize "to designers, manufacturers (both manufacturers of radioactive sources and manufacturers of devices in which radioactive sources are incorporated), suppliers and users and those managing disused sources **their responsibilities for the safety and security of radioactive sources**" (paragraph 15);
- To define "its **domestic threat**, and **assess its vulnerability** with respect to this threat for the variety of sources used within its territory, based on the potential for loss of control and malicious acts involving one or more radioactive sources" (paragraph 16);
- To have legislation and regulations in place for "requirements for **security measures to deter, detect, and delay** the unauthorized access to, or the theft, loss or unauthorized use or removal of radioactive sources during all stages of management" (paragraph 19);
- To ensure that "the regulatory body established by its legislation has the authority to attach clear and unambiguous conditions to the authorizations issued by it, including conditions relating to:…(viii) measures to determine, as appropriate, the **trustworthiness** of individuals involved in the management of radioactive sources; and (ix) the **confidentiality of information** relating to the security of sources" (paragraph 20);
- To ensure that its regulatory body has the authority to **require a security plan or assessment, as appropriate, and to promote the establishment of a security culture** among all individuals and in all bodies involved in the management of radioactive sources (paragraphs 20 and 22).

The characteristics of security culture are the beliefs, attitudes, behaviour and management systems, the proper assembly of which lead to more effective security.

The foundation of security culture is a recognition — by those that have a role in regulating, managing or operating facilities or activities involving radioactive sources, or even those that could be affected by these activities — that a credible threat exists and that security is important.

Readers of this guide should also read Nuclear Security Culture [14], which describes the basic concepts and elements of security culture.

Security culture may be enhanced by various means including, as appropriate:

— Assigning responsibility for the security of radioactive sources to a senior staff member, but ensuring that staff members are aware that security is a shared responsibility across the whole organization;
— Documenting legal and regulatory security responsibilities applying to the operator and bringing this to the attention of relevant managers, staff and, where appropriate, all employees and contractors;
— Ensuring threat awareness and training security managers, response personnel and all personnel with secondary responsibilities for security;
— Addressing security matters in staff and contractor induction courses;
— Providing security instructions and ongoing security awareness briefings to staff and contractors, and training and evaluation of the lessons learned;
— Conducting regular performance testing and preventive maintenance.

3.3. PURPOSE OF A SECURITY SYSTEM

A security system should be designed by the operator's security professionals to deter adversaries from committing a malicious act or to minimize through detection, delay and response the likelihood of an adversary succeeding in completing such a malicious act. Such an act would consist of a sequence of actions by one or more adversaries (threat) to obtain access to a source (target) either in order to commit an act of sabotage or another malicious act, or in order to remove the source without authorization.

3.4. SECURITY FUNCTIONS

A security system to protect radioactive sources from an adversary intent on committing a malicious act should be designed to perform basic security functions: deterrence, detection, delay, response, and security management:

— ***Deterrence*** occurs when an adversary, otherwise motivated to perform a malicious act, is dissuaded from undertaking the attempt. Deterrent measures have the effect of convincing the adversary that the malicious act would be too difficult, the success of the act too uncertain, or the consequence of the act to the adversary too unpleasant to justify the undertaking. Measures designed specifically to deter thus involve communication to the adversary about the presence of measures

performing the other security functions. If this communication has the intended effect, deterrence is the result.

— ***Detection*** is the discovery of an attempted or actual intrusion which could have the objective of unauthorized removal or sabotage of a radioactive source. Detection can be achieved by several means, including visual observation, video surveillance, electronic sensors, accountancy records, seals and other tamper indicating devices, process monitoring systems, and other means. Adversary awareness of detection measures can also serve as a deterrent.

— ***Delay*** impedes an adversary's attempt to gain unauthorized access or to remove or sabotage a radioactive source, generally through barriers or other physical means. A measure of delay is the factor of time, after detection, that is required by an adversary to remove or sabotage the radioactive source. Adversary awareness of delay barriers can also serve as a deterrent.

— ***Response*** encompasses the actions undertaken following detection to prevent an adversary from succeeding or to mitigate potentially severe consequences. These actions, typically performed by security or law enforcement personnel, and other State agencies, include interrupting and subduing an adversary while the attempted unauthorized removal or sabotage is in progress, preventing the adversary from using the radioactive source to cause harmful consequences, recovering the radioactive source, or otherwise reducing the severity of the consequences. The prospect of successful response can also serve as a deterrent.

— ***Security management*** includes ensuring adequate resources (personnel and funding) for the security of sources. It also includes developing procedures, policies, records, and plans for the security of sources and for a more effective security culture, in general. This term also includes developing procedures for the proper handling of sensitive information and protecting it against unauthorized disclosure.

3.5. DESIGN AND EVALUATION OF SECURITY SYSTEMS

A well designed security system should integrate measures to perform all five security functions so as to effectively secure the target from the threat, consistent with the following security concepts:

Deterrence cannot be measured: The objective of deterrence is to dissuade an adversary from attempting a malicious act. As a result, the impact of deterrent measures cannot be quantified. Therefore, the design of a security system should not be wholly based on deterrence.

Detection before delay: The function of delay is to provide response personnel with sufficient time to deploy and interrupt or interdict the adversary's efforts to complete a malicious act. Therefore, detection must precede delay. If an adversary is given the opportunity to overcome barriers and other obstacles prior to encountering intrusion sensors or other detection means, the adversary will have completed the most difficult tasks before being detected and thus may well succeed in removing or sabotaging the radioactive source before the response personnel arrive. In this case, barriers do not serve as a delay but rather, at most, as deterrents.

Detection requires assessment: Most means of detection provide an indirect indication of potential malicious action, such as attempted unauthorized access, removal or sabotage of a radioactive source. The only direct indication is by direct human observation. Therefore, when an alarm, or other indirect indication is triggered, there is always some uncertainty as to the cause. As a result, detection should always be complemented by assessment to determine the cause of the alarm. Alarm assessment requires human observation and judgment, through deployment of response personnel to investigate the cause of the alarm, through remote closed circuit television (CCTV) systems, or similar means. Sometimes, adversaries may attempt to exploit any delay between detection and assessment to mask their malicious intent. Therefore, immediate assessment is the goal of any security system.

Delay greater than assessment plus response time: A security system is successful if it detects and a correct assessment is made of an adversary attempting a malicious act in sufficient time for subsequent delay measures to permit response personnel to interrupt and stop the adversary prior to completion of the act or to initiate prompt actions to mitigate potentially high consequences. This relationship of the functions of detection, delay and response is known as *timely detection.*

Balanced protection: This is a concept of equivalent security functions (deterrence, detection delay, response, and security management) that provides adequate protection against all threats along all possible pathways. In other words, delay times through each pathway, detection measures associated with each detection element and the resulting responses provide the necessary protection to prevent a successful act.

Defence in depth: A concept of several layers and methods of protection (structural, technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve their objective.

3.6. INTEGRATION OF SAFETY AND SECURITY MEASURES

Safety measures and security measures have in common the aim of protecting human life and health and the environment. Safety measures and security measures should be designed and implemented in an integrated manner so that security measures do not compromise safety and safety measures do not compromise security. In implementing the recommendations in this guide, the designers of security systems should consult with qualified safety experts to ensure that security measures do not compromise the safety of individuals or the protection of the environment.

3.7. GRADED APPROACH TO SECURITY

Security requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness of a radioactive source, the nature of the source and potential consequences associated with its unauthorized removal or sabotage. This graded approach ensures that the highest consequence sources receive the greatest degree of security.

3.8. UNDERSTANDING AND ADDRESSING THE THREAT ENVIRONMENT

The design and evaluation of a security system should take into account the current national threat assessment and may include the development and application of a design basis threat (DBT) (see the Definitions).

3.8.1. National threat assessment

The Code of Conduct states:

> "Every State should define its domestic threat, and assess its vulnerability with respect to this threat for the variety of sources used within its territory, based on the potential for loss of control and malicious acts involving one or more radioactive sources."

The procedure for meeting this principle should begin with a national threat assessment, which is an analysis that documents at a national level the credible motivations, intentions, and capabilities of potential adversaries that

could cause harm through the sabotage of a facility or the unauthorized removal of a radioactive source for malicious purposes. Typically, such an assessment is conducted by a State's intelligence community, often with input from such agencies as ministries of interior, defence, transportation, and foreign affairs; law enforcement; customs and coast guard; and other agencies with security related responsibilities, and may include the regulatory body. If not previously involved in this assessment, the regulatory body should be informed of the threat as currently assessed by the relevant national agencies for use in the development of its regulatory programme for security of radioactive sources.

The assessment process is one of deductive reasoning. Starting from what is known, a judgment is made about how adversary groups or individuals may behave in the future. This would include, for example, historic events and known capabilities to attack the types of facilities where radioactive sources are stored or used. The threat assessment should cover at least the following attributes and characteristics for each identified insider and external adversary:

— *Motivation*. Political, financial, ideological, personal.
— *Level of commitment*. Disregard for personal health, safety, well-being, or survival.
— *Intentions*. Material or facility sabotage (unauthorized removal), public panic and disruption, political instability, mass injuries and casualties.
— *Group size*. Attack force, coordination, support.
— *Weapons*. Types, numbers, availability, improvised.
— *Tools*. Mechanical, thermal, manual, power, electronic, electromagnetic, communications equipment.
— *Modes of transport*. Public, private, land, sea, air, type, number, availability.
— *Technical skills*. Engineering, use of explosives and chemicals, paramilitary experience, communication skills.
— *Cyber skills*. Using computers and automated control systems in direct support of physical attacks, for intelligence gathering, for computer based attacks, for money collection, etc.
— *Knowledge*. Targets, site plans and procedures, security measures, safety and radiation protection procedures, operations, potential use of nuclear or other radioactive material.
— *Funding*. Source, amount, availability.
— *Insider issues*. Collusion, passive/active, violent/non-violent, number of insiders.
— *Support structure*. Local sympathizers, support organization, logistics;
— *Tactics*. Covert and overt.

Once the State has made an assessment of its threat, it will need to decide on a basis for establishing its regulations for the security of radioactive sources. One approach is to establish regulations on the basis of the national threat assessment while another is to regulate on the basis of the DBT (see below), for which the national threat assessment becomes an input. In selecting a regulatory basis, there are several factors that need to be considered by the State, including the severity of consequences associated with malicious acts involving radioactive sources in the State, determination by the State of the ability to establish effective protection systems using each approach, and the ability of the regulatory body to implement the different approaches.

It is worth noting that all States need not use a DBT approach for their regulatory system. However, if a DBT approach is not selected, the State will still need to prepare a national threat assessment and keep it current.

3.8.2. Design basis threat

A DBT, defined at the State level, is a tool used to help establish performance requirements for the design of physical protection systems for specific types of facilities. It is also used to help operators and State authorities assess the effectiveness of the systems to counter adversaries by evaluating the systems' performance against adversary capabilities described in the DBT, by conducting vulnerability assessments. A DBT is a comprehensive description of the motivations, intentions and capabilities of potential adversaries against which protection systems are designed and evaluated. The capabilities of the adversary, whether an insider or external, help determine the detection, delay, and response requirements for a physical protection system to be effective against a DBT.

The development of a DBT will be specific to each State, due to social, cultural and geopolitical differences. As with the national threat assessment, developing a DBT typically requires the combined efforts of domestic authorities such as intelligence and security agencies, law enforcement and regulatory bodies and operators. The DBT may need to be reviewed from time to time in the light of new information from State organizations. More detailed information on the DBT process can be found in Ref. [13].

3.8.3. Insider threats

Insider threats should be given particular attention when designing a security system. Such threats could stem from one or more persons with legitimate access to a facility and detailed knowledge of activities or source locations. These individuals may be employees or contractors who could

remove radioactive sources or information, with malicious intent, or conduct acts of sabotage on the premises. Moreover, individuals may seek employment at a facility with the intention of committing malicious acts and may also assist external adversaries to remove sources or carry out hostile acts. Insider threats and recommended appropriate countermeasures are further explained in Ref. [15].

3.8.4. Increased threat

A security system should be effective in countering the currently assessed threat. However, there should be provisions to ensure that the security status can be temporarily heightened during times of increased threat. This should include the introduction of additional security measures or reduction in the accessibility to the radioactive sources.

3.9. VULNERABILITY ASSESSMENT

A vulnerability assessment (VA), also known as a security survey or security assessment, is a method for evaluating protective security systems. It is a systematic appraisal of the effectiveness of a security system for protection against an assessed threat (or DBT if one exists). The VA can be specific or general in nature, can be conducted locally by the operator or by the State/regulatory body, and can be used to help the development of regulations by the State/regulatory body or for demonstrating regulatory compliance of the operator. Additional information on how to perform a VA can be found in Appendix III.

4. ESTABLISHING A REGULATORY PROGRAMME FOR RADIOACTIVE SOURCE SECURITY

The provisions in the Code of Conduct relating to the security of radioactive sources have been strengthened to provide measures to reduce the likelihood of malicious acts. The Code also specifically mentions that States should give appropriate attention to radioactive sources considered by them to have the potential to cause unacceptable consequences if employed for malicious purposes. In case of such an event, requirements and guidance on

emergency preparedness and response, intervention and the remediation of contaminated areas are available from the IAEA [5, 9, 10]. Guidance on protecting people against radiation in the aftermath of a radiological attack is given by the International Commission on Radiological Protection [11].

Such malicious acts and potential consequences could include:

- The deliberate placement of a breached or unshielded source in a public area;
- The deliberate dispersion of radioactive material to cause adverse health effects (by using, for example, a radioactive dispersal device (RDD));
- The use of an RDD for the purposes of contaminating ground, buildings and infrastructure leading to denial of access to these areas, which may be based on radiation protection criteria, economic impact and the cost of clean up and reconstruction.

Many States already have a regulatory programme in place that covers activities such as authorization, review and assessment, inspection and enforcement [16]. This section provides guidance to regulatory bodies on how to develop or enhance regulatory programmes to address the security of radioactive sources in order to reduce the likelihood of malicious acts involving those sources. Safety and security measures should be designed and implemented in an integrated manner so that they do not compromise each other.

Establishing such a regulatory programme for the security of radioactive sources involves three basic steps for the regulatory body:

- **Step 1:** Establish graded security levels with corresponding goals and objectives for each security level (see Section 4.1).

- **Step 2:** Determine the security level applicable to a given source (see Section 4.2).

- **Step 3:** Select and implement a regulatory approach (prescriptive, performance based, or combined) for directing operators as to how to design, implement and evaluate security measures in order to meet the security objectives in Table 1 (see Section 4.3).

4.1. STEP 1: ESTABLISH GRADED SECURITY LEVELS WITH CORRESPONDING GOALS AND OBJECTIVES

Radioactive sources have a wide range of characteristics (such as activity) that make them attractive in varying degrees to adversaries. A corresponding range of effective security measures should be utilized to ensure that the sources are adequately protected using a graded approach. In order to ensure adequate security capability without imposing overly restrictive measures, the concept of security levels should be used. Three security levels (A, B, and C) have been developed to allow specification of security system performance in a graded manner. Security level A requires the highest degree of security while the other levels are progressively lower.

Each security level has a corresponding goal. The goal defines the overall result that the security system should be capable of providing for a given security level. The following goals have been developed:

- **Security level A**: *Prevent* unauthorized removal of a source.
- **Security level B**: *Minimize the likelihood* of unauthorized removal of a source.
- **Security level C**: *Reduce the likelihood* of unauthorized removal of a source.

Malicious acts can involve either unauthorized removal of a source or sabotage. While the security goals only address unauthorized removal, achievement of the goals will reduce the likelihood of a successful act of sabotage. Security systems that achieve the goals listed above will provide some (although limited) capability to detect and respond to an act of sabotage.

In order to meet the *goals*, it is necessary to achieve an adequate level of performance for each of the security *functions*: deterrence, detection, delay, response, and security management. That level of performance is defined as a set of *objectives* for each of the functions. These objectives state the desired outcome from the combination of *measures* applied for that objective. Deterrence is a security function which is difficult to quantify. Consequently, it has not been assigned an associated set of security objectives and measures in this publication.

Security levels and associated security objectives are summarized in Table 2.

Where an objective is shown in Table 2 as the same for two or more security levels, it is intended that the objective be met in a more rigorous manner for the higher security level.

TABLE 2. SECURITY LEVELS AND SECURITY OBJECTIVES

Security functions	Security objectives		
	Security Level A Goal: Prevent unauthorized removal[a]	Security Level B Goal: Minimize likelihood of unauthorized removal[a]	Security Level C Goal: Reduce likelihood of unauthorized removal[a]
Detect	Provide immediate detection of any unauthorized access to the secured area/source location		
	Provide immediate detection of any attempted unauthorized removal of the source, including by an insider	Provide detection of any attempted unauthorized removal of the source	Provide detection of unauthorized removal of the source
	Provide immediate assessment of detection		
	Provide immediate communication to response personnel		
	Provide a means to detect loss of source through verification		
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal	Provide delay to minimize the likelihood of unauthorized removal	Provide delay to reduce the likelihood of unauthorized removal
Response	Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal	Provide immediate initiation of response to interrupt the unauthorized removal	Implement appropriate action in the event of unauthorized removal of a source
Security management	Provide access controls to source location that effectively restrict access to authorized persons only		
	Ensure trustworthiness of authorized individuals		
	Identify and protect sensitive information		
	Provide a security plan		
	Ensure a capability to manage security events covered by security contingency plan (see the Definitions)		
	Establish security event reporting system		

[a] Achievement of these goals will also reduce the likelihood of a successful act of sabotage.

4.2. STEP 2: DETERMINE THE SECURITY LEVEL APPLICABLE TO A GIVEN SOURCE

In order to specify an appropriate security level for a source, consideration should be given to the potential harm that the source could cause if it were used in a malicious act. This potential for harm then guides the process of assigning an appropriate security level to the source. This process consists of the following steps:

— Categorizing sources based on the potential to cause harm if used for malicious purposes (including aggregation of sources in a given location as appropriate) (see Section 4.2.1);
— Assigning an appropriate security level to each category (see Section 4.2.2).

4.2.1. Categorization of radioactive sources

The Code of Conduct applies to radioactive sources that may pose a significant risk to individuals, society, and the environment, i.e. sources in Categories 1–3. Appropriate security measures should be applied to reduce the likelihood of malicious acts involving these sources.

The source categorization used in the Code of Conduct is based on the concept of 'dangerous sources' which are quantified in terms of D values [17]. This concept is further discussed in the IAEA's Categorization of Radioactive Sources [3]. This publication provides a recommended system of categorization, particularly for those sources used in industry, medicine, agriculture, research and education. This system of categorization can also be applied, where appropriate, in the national context, to sources within military or defence programmes. The categorization provides an internationally harmonized basis for risk informed decision making and is based on a logical and transparent method that provides the flexibility for it to be applied in a wide range of circumstances. The risk informed decisions can be made in a graded approach to the regulatory control of radioactive sources for the purposes of safety and security.

In recognition of the fact that human health is of paramount importance, the categorization system is based primarily on the potential for radioactive sources to cause deterministic health effects. The D value is the radionuclide specific activity of a source which, if not under control, could cause severe deterministic effects for a range of scenarios that include both external exposure from an unshielded source and inadvertent internal exposure following dispersal (e.g. by fire or explosion) of the source.

The activity of the radioactive material (A) in sources varies over many orders of magnitude; D values are therefore used to normalize the range of activities in order to provide a reference in comparing risks. This should be done by taking the activity A of the source (in TBq) and dividing it by the D value for the relevant radionuclide.

It should be noted that there is the potential for amounts of material less than the D values to be dangerous [17]. This could be the case in the event of malicious administration of unsealed radioactive material to an individual.

The activity thresholds for radionuclides in the Code of Conduct for source Categories 1–3 are listed in Table 3. For radionuclides not found in this table, please see Refs. [3, 17].

In some situations it may be appropriate to categorize a source on the basis of A/D alone, e.g. when intended use of the source is unknown or not confirmed. However, when the circumstances of use of the source are known, the regulatory body may make a judgment to modify this initial categorization using other information about the source or its use. In some circumstances it may be convenient to assign a category on the basis of the intended use of the source (see Table 4).

The categorization system has five categories, as shown in Table 4. This number of categories should be sufficient to enable the practical applications of the scheme, without unwarranted precision. Within this categorization system, sources in Category 1 are considered to be the most 'dangerous' because they can pose a very high risk to human health if not managed safely and securely. An exposure of only a few minutes to an unshielded Category 1 may be fatal. At the lower end of the categorization system, sources in Category 5 are the least dangerous; however, even these sources could give rise to doses in excess of the dose limits if not properly controlled, and therefore should be kept under appropriate regulatory control. Categories should not be subdivided as this would imply a degree of precision that is not warranted and could lead to a loss of international harmonization.

4.2.1.1. Unlisted sources

For radioactive sources not listed in Table 4, the regulatory body may assign a category to the source based on the A/D ratio.

4.2.1.2. Short half-life radionuclides

In some activities, such as nuclear medicine, radionuclides with a short half-life are used in a source form that is unsealed. Examples of such

TABLE 3. ACTIVITIES CORRESPONDING TO THRESHOLDS OF CATEGORIES

Radionuclide	Category 1 1000 ×D		Category 2 10 ×D		Category 3 D	
	(TBq)	(Ci)[a]	(TBq)	(Ci)[a]	(TBq)	(Ci)[a]
Am-241	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Am-241/Be	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Cf-252	2.E+01	5.E+02	2.E-01	5.E-00	2.E-02	5.E-01
Cm-244	5.E+01	1.E+03	5.E-01	1.E+01	5.E-02	1.E+00
Co-60	3.E+01	8.E+02	3.E-01	8.E+00	3.E-02	8.E-01
Cs-137	1.E+02	3.E+03	1.E+00	3.E+01	1.E-01	3.E+00
Gd-153	1.E+03	3.E+04	1.E+01	3.E+02	1.E+00	3.E+01
Ir-192	8.E+01	2.E+03	8.E-01	2.E+01	8.E-02	2.E+00
Pm-147	4.E+04	1.E+06	4.E+02	1.E+04	4.E+01	1.E+03
Pu-238	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Pu-239[b]/Be	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Ra-226	4.E+01	1.E+03	4.E-01	1.E+01	4.E-02	1.E+00
Se-75	2.E+02	5.E+03	2.E+00	5.E+01	2.E-01	5.E+00
Sr-90 (Y-90)	1.E+03	3.E+04	1.E+01	3.E+02	1.E+00	3.E+01
Tm-170	2.E+04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02
Yb-169	3.E+02	8.E+03	3.E+00	8.E+01	3.E-01	8.E+00
Au-198*	2.E+02	5.E+03	2.E+00	5.E+01	2.E-01	5.E+00
Cd-109*	2.E+04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02
Co-57*	7.E+02	2.E+04	7.E+00	2.E+02	7.E-01	2.E+01
Fe-55*	8.E+05	2.E+07	8.E+03	2.E+05	8.E+02	2.E+04
Ge-68*	7.E+02	2.E+04	7.E+00	2.E+02	7.E-01	2.E+01
Ni-63*	6.E+04	2.E+06	6.E+02	2.E+04	6.E+01	2.E+03
Pd-103*	9.E+04	2.E+06	9.E+02	2.E+04	9.E+01	2.E+03
Po-210*	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Ru-106 (Rh-106)*	3.E+02	8.E+03	3.E+00	8.E+01	3.E-01	8.E+00
Tl-204*	2.E+04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02

[a] The primary values to be used are given in TBq. Curie values are provided for practical usefulness and are rounded after conversion.

[b] Criticality and safeguards issues will need to be considered for multiples of D.

* These radionuclides are very unlikely to be used in individual radioactive sources with activity levels that would place them within Categories 1, 2 or 3 and would, therefore, not be subject to those paragraphs of the Code relating to national registries or to import and export controls.

TABLE 4. CATEGORIES FOR COMMONLY USED SOURCES

Category	Source[a]	A/D[b]
1	Radioisotope thermoelectric generators (RTGs) Irradiators Teletherapy sources Fixed multibeam teletherapy (gamma knife) sources	$A/D \geq 1000$
2	Industrial gamma radiography sources High/medium dose rate brachytherapy sources	$1000 > A/D \geq 10$
3	Fixed industrial gauges that incorporate high activity sources[c] Well logging gauges	$10 > A/D \geq 1$
4	Low dose rate brachytherapy (except eye plaques and permanent implants) Industrial gauges that do not incorporate high activity sources Bone densitometers Static eliminators	$1 > A/D \geq 0.01$
5	Low dose rate brachytherapy eye plaques and permanent implant sources X ray fluorescence (XRF) devices Electron capture devices Mossbauer spectrometry sources Positron emission tomography (PET) check sources	0.01 > A/D and A > exempt[d]

[a] Factors other than A/D alone have been taken into consideration in assigning the sources to a category (see Ref. [3], Annex I).

[b] This column can be used to determine the category of a source purely on the basis of A/D. This may be appropriate, for example, if the facilities and activities are not known or are not listed, if sources have a short half-life and/or are unsealed, or if sources are aggregated (see Ref. [3], paragraph 3.5).

[c] Examples are given in Ref. [3], Annex I.

[d] Exempt quantities are given in Schedule I of Ref. [5].

applications include ^{99m}Tc in radiodiagnosis and ^{131}I in radiotherapy. In such situations, the principles of the categorization system may be applied to determine a category for the source. These situations should be considered on a case by case basis.

4.2.1.3. Unsealed radioactive sources

The regulatory body may assign a category to unsealed radioactive sources based on the A/D ratio.

4.2.1.4. Radioactive decay

If the activity of a source decays to a level below the appropriate threshold in Table 3 or below that which is normally used (as shown in Table 4), the regulatory body may allow the operator to recategorize the source based on the A/D ratio.

4.2.1.5. Aggregation of sources

There will be situations in which radioactive sources are in close proximity, such as in manufacturing processes (e.g. in the same room or building) or in storage facilities (e.g. in the same enclosure). In such circumstances, the regulatory body may wish to aggregate the activity in the sources to determine a situation specific categorization for the purposes of implementing regulatory control measures. In situations of this type, the summed activity of the radionuclide should be divided by the appropriate D value and the calculated ratio A/D compared with the ratios of A/D given in Table 2, thus allowing the set of sources to be categorized on the basis of activity. If sources with various radionuclides are aggregated, then the sum of the ratios A/D should be used in determining the category, in accordance with the formula:

$$\text{Aggregate A/D} = \sum_n \frac{\sum_i A_{i,n}}{D_n}$$

where:

$A_{i,n}$ = activity of each individual source i of radionuclide n.
D_n = D value for radionuclide n.

Additional information on the aggregation of radioactive sources may be found in Ref. [3].

4.2.2. Assigning security levels

As a default arrangement, the regulatory body could use the categories listed above to assign the security level applicable to a given source.

Category 1 sources should have security measures which meet the security objectives of Security Level A. Category 2 sources should have security measures which meet the security objectives of Security Level B. Category 3 sources should have security measures which meet the security objectives of Security Level C.

The International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources (paragraph 2.34 [5]) include general requirements for the security of radioactive sources. This guide considers that while those control measures provide a sufficient level of security for radioactive sources in Categories 4 and 5, enhanced measures specified in this guide should be applied to radioactive sources in Categories 1, 2 and 3 in order to reduce the likelihood of malicious acts involving those sources. Furthermore, the regulatory body, taking account of its national threat, may wish to enhance the security of sources in Categories 4 and 5 sources in appropriate circumstances. This approach is summarized in Table 5.

While this approach can be viewed as a default position, the malicious use of radioactive sources may not necessarily involve sources that are ranked highest in this categorization scheme. Most Category 1 sources, for example, will be held within shielding and inside fixed devices or facilities. Efforts to remove the source would take time and may expose the adversaries to a significantly harmful level of radiation. It is, therefore, possible that adversaries will focus on sources of a lower category, more accessible, less of a hazard to handle, portable, and more easily concealed.

The purpose of categorizing radioactive sources is to provide an internationally accepted basis for risk informed decision making, including measures to reduce the likelihood of malicious acts. However, socioeconomic consequences resulting from malicious acts were excluded from the categorization criteria as no methodology for quantifying and comparing these consequences exists, especially on an international basis.

4.2.3. Additional considerations for assigning security levels

Annex I of the Code of Conduct notes that States should give appropriate attention to radioactive sources considered by them to have the potential to cause unacceptable consequences if employed for malicious purposes.

Although Refs [3, 17] already take into account some of the factors below, the regulatory body needs to pay special attention to these factors and

TABLE 5. RECOMMENDED DEFAULT SECURITY LEVELS FOR COMMONLY USED SOURCES

Category	Source	A/D	Security level
1	RTGs Irradiators Teletherapy sources Fixed multibeam teletherapy (gamma knife) sources	A/D ≥ 1000	A
2	Industrial gamma radiography sources High/medium dose rate brachytherapy sources	1000 > A/D ≥ 10	B
3	Fixed industrial gauges that incorporate high activity sources Well logging gauges	10 > A/D ≥ 1	C
4	Low dose rate brachytherapy (except eye plaques and permanent implants) Industrial gauges that do not incorporate high activity sources Bone densitometers Static eliminators	1 > A/D ≥ 0.01	Apply measures as described in the Basic Safety Standards [5]
5	Low dose rate brachytherapy eye plaques and permanent implant sources XRF devices Electron capture devices Mossbauer spectrometry sources Positron emission tomography (PET) check sources	0.01 > A/D and A > exempt	

considerations when assigning security levels to radioactive sources. These factors represent variables that are specific to the source and the manner and location in which it is used — and these may affect the level of security that is appropriate for a given source or facility.

4.2.3.1. Attractiveness of sources

In addition to the activity of a source, there are other factors that may make some sources more attractive for use in malicious acts. These factors include:

- The chemical and physical form of the radioactive material in the source, which may make it easily dispersible and hence more attractive to an adversary.
- The nature of the radioactive emission. Some radionuclides produce higher doses per unit intake than others, notably alpha emitters. Sources containing these radionuclides may be more attractive for use in an RDD.
- Ease of handling. Sources that can be easily handled or are easily accessible may be more attractive since the adversary will be less likely to receive a high radiation dose and the source is more easily moved. An example of this is a source inside a self-shielded portable device.
- Co-location. Multiple sources or large quantities of radioactive material that are co-located may be attractive to an adversary since successful penetration of the security system may allow removal or sabotage of sufficient material to produce very serious consequences.
- Perceived economic value of the source or the equipment it may be inside.

The regulatory body may wish to consider the attractiveness of sources in determining the security level assigned to a source and the security measures applied to that security level.

4.2.3.2. Sources in storage

Radioactive sources placed in storage should be protected in accordance with the measures reflected in this publication and according to the categorization and security level applied to the source.

4.2.3.3. Vulnerability and threat level

The domestic threat level and any increases in it may warrant evaluation of the security level assigned to a source, taking into account all other attributes of the source (e.g. attractiveness, vulnerability). Alternatively, specific security measures for a given security level may also be strengthened.

4.2.3.4. Mobile, portable and remote sources

Sources used in field applications (e.g. radiography and well logging) are typically contained in devices designed for portability and are frequently transported between job sites. The ease of handling of these devices and their presence in vehicles outside secured facilities make them attractive for unauthorized removal.

Recognizing that security measures for fixed sources may not be practical for application to sources used in the field, alternative measures should be applied to achieve the security objective. Please refer to the detection and delay measures for Security Levels B and C (Section 4.3.1), as well as the illustrative security measures for mobile sources in Appendix IV.

Sources that are used in remote locations could be removed by unauthorized personnel and transported out of the area before effective response is possible.

The regulatory body may wish to consider mobility, portability and location when assigning a security level to a source or may wish to consider additional measures within the assigned security level to compensate for these conditions.

4.3. STEP 3: SELECT AND IMPLEMENT A REGULATORY APPROACH

There are three alternative approaches that the regulatory body may use for directing operators on how to demonstrate that they meet the security objectives specified in Table 2. The approach(es) selected by the regulatory body should take into account its own capabilities and resources, the capabilities and resources of the operators that it regulates, and the range of sources that should be protected:

— A *prescriptive approach* establishes specific security measures determined by the regulatory body to meet the security objectives for each security level. The guidance in this section identifies a set of such measures for each security level, which the regulatory body may adopt as requirements in the absence of a DBT. Alternatively, the regulatory body may use the security measures in this guidance as a starting point, but tailor them to national circumstances. Use of the prescriptive approach is particularly appropriate in cases where the combination of threat and potential consequences is low or where conducting a detailed threat assessment is not possible. The prescriptive approach has the advantage

of simplicity in implementation for both the regulatory body and operators, and also ease of inspection and auditing. The disadvantage of this approach is its relative lack of flexibility to address actual circumstances. For example, experience has shown that an operator can be in compliance with prescribed measures, and yet not meet the aim of the security system to protect the targets from the actual or defined threat. Consequently, when the prescriptive approach is used, the regulatory body needs to ensure that inspections or security assessments are performed to evaluate the overall effectiveness of the facility's security system in meeting the security goal and objectives for the applicable security level (see Section 4.3.1).

— A *performance based approach* is one where the regulatory body allows flexibility for the operator to propose the particular combination of security measures that will be used to achieve the security objectives in Table 2. The proposed security measures should be based on vulnerability assessment, taking into account information provided by the regulatory body, based on a national threat assessment and, where applicable, a DBT. The advantages of this approach are that it recognizes that an effective security system can be composed of many combinations of security measures, and that each operator's circumstances can be unique. The prerequisite for this approach is that it requires both the operator and the regulatory body to have relatively high levels of security expertise (see Section 4.3.2).

— A *combined approach* includes elements drawn from both prescriptive and performance based approaches. There are many possible versions of the combined approach. For example, the regulatory body may adopt a set of security measures from which the operator may choose, while requiring the operator to demonstrate that the security system as a whole meets the applicable security objectives. Alternatively, the regulatory body could use a performance-based approach for the radioactive sources with the highest potential consequences of malicious use and a prescriptive approach for lower consequence sources. Or, a set of prescriptive requirements could be supplemented with performance-oriented requirements addressing particular matters. The main advantage of the combined approach is the flexibility it allows (see Section 4.3.3).

The remainder of this section provides guidance to regulatory bodies for using each approach.

4.3.1. Prescriptive approach

The regulatory body may choose to specify security measures that operators are required to have in place in order to meet the security objectives in Table 2. Tables 6, 7 and 8 specify security measures intended to meet the security objectives of Security Levels A, B and C, respectively. These tables include security measures for sources in use or in storage. The measures are discussed in detail after each corresponding table. The measures may vary depending on whether a given source is in use or in storage, or is a mobile or portable source. More information on some of these measures can be found in Appendix I. Illustrative security measures that may be applied to selected facilities and activities are provided in Appendix IV.

Introduction for Security Level A measures

The goal of Security Level A is to **prevent the unauthorized removal** of radioactive sources. If an attempt at unauthorized access or unauthorized removal were to occur, detection and assessment have to occur early enough to enable response personnel to respond with enough time and with sufficient resources to interrupt the adversary and prevent the source from being removed. In order to achieve this goal, the following measures are recommended.

Detection

Security objective: Provide immediate detection of any unauthorized access to the secured area/source location.

Security measures: Electronic intrusion detection system and/or continuous surveillance by operator personnel.

Electronic sensors linked to an alarm or continuous visual surveillance by operator personnel indicate unauthorized access to the secured area (see the section on 'Delay' below) or source location. Care should be taken to ensure that intrusion detection measures cannot be bypassed. For sources in use, such measures should detect unauthorized access to the secured area where the source is used. For sources in storage, such measures should detect unauthorized access to the locked room or other location where the source is stored. For mobile or portable sources in use, continuous visual surveillance may be the only feasible means of immediate intrusion detection.

TABLE 6. RECOMMENDED MEASURES FOR SECURITY LEVEL A
(goal: prevent unauthorized removal)

Security function	Security objective	Security measures
Detect	Provide immediate detection of any unauthorized access to the secured area/source location.	Electronic intrusion detection system and/or continuous surveillance by operator personnel.
	Provide immediate detection of any attempted unauthorized removal of the source, including by an insider.	Electronic tamper detection equipment and/or continuous surveillance by operator personnel.
	Provide immediate assessment of detection.	Remote monitoring of CCTV or assessment by operator / response personnel.
	Provide immediate communication to response personnel.	Rapid, dependable, diverse means of communication such as phones, cell phones, pagers, radios.
	Provide a means to detect loss through verification.	Daily checking through physical checks, CCTV, tamper indicating devices, etc.
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal.	System of at least two layers of barriers (e.g. walls, cages) which together provide delay sufficient to enable response personnel to interdict
Response	Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal.	Capability for immediate response with size, equipment, and training to interdict.
Security management	Provide access controls to source location that effectively restrict access to authorized persons only.	Identification and verification, for example, lock controlled by swipe card reader and personal identification number, or key and key control.
	Ensure trustworthiness of authorized individuals.	Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information.
	Identify and protect sensitive information.	Procedures to identify sensitive information and protect it from unauthorized disclosure
	Provide a security plan.	A security plan which conforms to regulatory requirements and provides for response to increased threat levels.
	Ensure a capability to manage security events covered by security contingency plans.	Procedures for responding to security-related scenarios.
	Establish security event reporting system.	Procedures for timely reporting of security events.

Security objective: Provide immediate detection of any attempted unauthorized removal of the source (e.g. an insider).

Security measures: Electronic tamper detection equipment and/or continuous surveillance by operator personnel.

Electronic sensors linked to an alarm or continuous visual surveillance by operator personnel indicate attempted unauthorized removal of a source. Care should be taken to ensure that tamper detection measures cannot be bypassed. For mobile sources in use, continuous visual surveillance may be the only feasible means of detecting attempted unauthorized removal. Note, however, that if continuous surveillance is chosen as a security measure, continuous visual surveillance may require observation by at least *two* individuals at all times to protect against an insider scenario.

Security objective: Provide immediate assessment of detection.

Security measures: Remote monitoring of CCTV or assessment by operator/ response personnel.

Once an intrusion detection or tamper detection alarm has been triggered, there should be an immediate assessment of the cause of the alarm. Assessment can be performed by operator personnel at the source location, through CCTV or by persons immediately deployed to investigate the cause of the alarm. For mobile or portable sources in use, or in other instances where intrusion detection or tamper detection is provided by continuous visual surveillance by operator personnel, assessment should be performed concurrently with detection by the operator personnel keeping the source under continuous visual surveillance.

Security objective: Provide immediate communication to response personnel.

Security measures: Rapid, dependable, diverse means of communication such as phones, cell phones, pagers, radios.

If the assessment confirms that unauthorized access or attempted unauthorized removal has occurred, immediate notification should be made to response personnel by operator personnel with diverse (at least two) means of communication such as landline telephones, auto-dialers, cellular phones, radios or paging devices.

Security objective: Provide a means to detect loss through verification.

Security measures: Daily checking through physical checks, CCTV, tamper indicating devices, etc.

Daily checking should consist of measures to ensure that the sources are present and have not been tampered with. Such measures could include physical checks that the source is in place, remote observation through CCTV, verification of seals or other tamper evident devices, and measurements of radiation or other physical phenomena that would provide an assurance that the source is present. For sources in use, verifying that the device is functional may be sufficient.

Delay

Security objective: Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal.

Security measures: System of least two layers of barriers (e.g. walls, cages) which together provide delay sufficient to enable response personnel to interdict.

A balanced system comprising at least two barriers should separate the source from unauthorized personnel and provide sufficient delay following detection to enable response personnel to intercede before the adversary can remove the source. For sources in use, such measures may include a locked device in a secured area to separate the device from unauthorized personnel. For sources in storage, such measures may include a locked and fixed container or a device holding the source in a locked storage room, thus separating the container from unauthorized personnel. For mobile sources in use, continuous visual surveillance by operator personnel may substitute for one or both layers of barriers.

Response

Security objective: Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal.

Security measures: Capability for immediate response with size, equipment, and training to interdict.

The operator should establish protocols to ensure immediate deployment of response personnel without delay in response to an alarm. The response should be both immediate and adequate. *Immediate* means that responders should arrive, once notified, in a time shorter than the time required to breach the barriers and perform the tasks needed to remove the source. *Adequate* means that the response team is of sufficient size and capability to subdue the adversary. Response may be a directly employed security force, a third party security team, local police, or national gendarmerie.

Security management

Security objective: Provide access controls to source location that effectively restrict access to authorized persons only.

Security measures: Identification and verification, for example, lock controlled by swipe card reader and personal identification number, or key and key control.

Access control is intended to limit access to the source location to authorized persons, generally by allowing such persons to temporarily disable physical barriers such as a locked door (delay measures) upon verification of the person's identity and access authorization. (In the context of medical exposure, patients do not need to be 'authorized' since they are escorted to the source and are under constant surveillance by the medical staff.)

The identity and authorization of a person seeking access can be verified by such measures as:

— Personal identification number (PIN) to activate a door control reader;
— A badge system which may also activate an electronic reader;
— A badge exchange scheme at an entry control point;
— Biometric features to activate a door control device.

Upon verification of a person's access authorization, the system allows that person to enter the secured area or source location, e.g. by opening a lock. A combination of two or more verification measures should be required, e.g. the use of a swipe card and a PIN; or the use of a swipe card and a controlled key; or a PIN and a computer password; or the use of a controlled key and visual verification of identity by other authorized personnel. For sources in use, such measures should control access to the area where the source is used. For sources in storage, such measures should control access to the locked room or other location where the source is stored. For mobile sources in use, continuous

visual surveillance by multiple operator personnel may substitute for access control.

Security objective: Ensure trustworthiness of authorized individuals.

Security measures: Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information.

An individual's trustworthiness should be assessed through a satisfactory background check before that person is allowed unescorted access to radioactive sources, locations where they are used or stored or any sensitive, related information. The nature and depth of background checks should be in proportion to the security level of the radioactive source and in accordance with the State's regulations or as determined by the regulatory body. As a minimum, background checks should involve confirmation of identity and the verification of references to determine the integrity, character and reliability of each person. The process should be periodically reviewed and supported through ongoing attention by supervisors and managers to ensure that personnel at all levels continue to act responsibly and reliably and any concerns, in this context, are made known to the relevant authority.

Security objective: Identify and protect sensitive information.

Security measures: Procedures to identify sensitive information and protect it from unauthorized disclosure.

As well as providing security of radioactive sources, it is necessary to protect related information, which may include documents, data on computer systems and other media that can be used to identify details of:

— The specific location and inventory of sources;
— The relevant security plan and detailed security arrangements;
— Security systems (e.g. intruder alarms) including performance and installation diagrams;
— Temporary or longer term weaknesses in the security programme;
— Security staffing arrangements and the means of response to events or alarms;
— Planned dates, routes and mode of shipment or transfer of sources;
— Contingency plans and security response measures.

Regulatory guidance should also provide for:

— Control, storage, preparation, identification, marking and transmission of documents or correspondence containing the sensitive information;
— Recommended methods for the destruction of documents containing sensitive information;
— Arrangements covering the declassification and management of documents when they are obsolete or no longer sensitive.

Security objective: Provide a security plan.

Security measures: A security plan which conforms to regulatory requirements and provides for response to increased threat levels.

A security plan should be prepared for each facility by its operator. For examples of content of a security plan, see Appendix II. Security plans may be authorized by the regulatory body and reviewed at prescribed intervals during the inspection process to ensure that they reflect the current security system. Security plans may be different for mobile and portable use sources, or for sources stored between periods of use. Most plans are likely to contain sensitive information about protective security arrangements and should therefore be managed accordingly. The security plan should also allow for an efficient and prompt transition to an enhanced level of security, in the case of an increase in the security threat.

Security objective: Ensure a capability to manage security events covered by security contingency plans

Security measures: Procedures for responding to security-related scenarios

At each facility security contingency plans should be drawn up for a range of events, including:

— A suspected or threatened malicious act;
— A public demonstration which has the potential to threaten the security of sources;
— An intrusion into the secured area by unauthorized person(s). This could range from simple trespass to a determined attack by those seeking to remove or interfere with radioactive sources.

The operator should develop reasonably foreseeable scenarios involving such events and procedures for responding to them. Security contingency plans should be shared with appropriate authorities and exercised at regular intervals.

Security objective: Establish security event reporting system.

Security measures: Procedures for timely reporting of security events.

The operator should develop procedures for reporting of security events to the regulatory body, first responders, and others as appropriate within a time frame required by the regulatory body commensurate with the security significance of the event. Events to be reported may include:

— Discrepancy in accounting data;
— Suspected or actual theft of a radioactive source;
— Unauthorized intrusion into a facility or source storage area;
— The discovery of a suspected or actual explosive device in or near a facility or store;
— Loss of control over a radioactive source;
— Unauthorized access to or unauthorized use of a source;
— Other malicious acts that threaten authorized activities;
— Suspicious events or sightings which might indicate planning for a sabotage attack, an intrusion or removal of a source;
— Failure or loss of security systems that are essential to the protection of radioactive sources.

TABLE 7. RECOMMENDED MEASURES FOR SECURITY LEVEL B
(goal: minimize the likelihood of unauthorized removal)

Security function	Security objective	Security measures
Detect	Provide immediate detection of any unauthorized access to the secured area/source location	Electronic intrusion detection equipment and/or continuous surveillance by operator personnel
	Provide detection of any attempted unauthorized removal of the source	Tamper detection equipment and/or periodic checks by operator personnel

TABLE 7. RECOMMENDED MEASURES FOR SECURITY LEVEL B
(goal: minimize the likelihood of unauthorized removal) (cont.)

Security function	Security objective	Security measures
	Provide immediate assessment of detection	Remote monitoring of CCTV or assessment by operator / response personnel
	Provide immediate communication to response personnel	Rapid, dependable means of communication such as phones, cell phones, pagers, radios
	Provide a means to detect loss through verification	Weekly checking through physical checks, tamper detection equipment, etc.
Delay	Provide delay to minimize the likelihood of unauthorized removal	System of two layers of barriers (e.g. walls, cages)
Response	Provide immediate initiation of response to interrupt unauthorized removal	Equipment and procedures to immediately initiate response
Security management	Provide access controls to source location that effectively restrict access to authorized persons only	One identification measure
	Ensure trustworthiness of authorized individuals	Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information
	Identify and protect sensitive information	Procedures to identify sensitive information and protect it from unauthorized disclosure
	Provide a security plan	A security plan which conforms to regulatory requirements and provides for response to increased threat levels
	Ensure a capability to manage security events covered by security contingency plans	Procedures for responding to security-related scenarios
	Establish security event reporting system	Procedures for timely reporting of security events

Introduction for Security Level B measures

The goal of Security Level B is to **minimize the likelihood of unauthorized removal** of radioactive sources. If an attempt of unauthorized access or unauthorized removal were to occur, the response must be initiated immediately upon detection and assessment of the intrusion, but the response is not required to arrive in time to prevent the source from being removed. In order to achieve this goal, the following measures are recommended.

Detection

Security objective: Provide immediate detection of any unauthorized access to the secured area/source location.

Security measures: Electronic intrusion detection equipment and/or continuous surveillance by operator personnel.

Electronic sensors linked to an alarm or continuous visual surveillance by operator personnel indicate unauthorized access to the secured area (see section on 'Delay' below) or source location. Care should be taken to ensure that intrusion detection measures cannot be bypassed. For sources in use, such measures should detect unauthorized access to the secured area where the source is used. For sources in storage, such measures should detect unauthorized access to the locked room or other location where the source is stored. For mobile or portable sources in use, continuous visual surveillance may be the only feasible means of intrusion detection.

Security objective: Provide detection of any attempted unauthorized removal of the source.

Security measures: Tamper detection equipment and/or periodic checks by operator personnel.

Tamper detection equipment or visual surveillance by operator personnel made during periodic checks indicate attempted unauthorized removal of a source. Care should be taken to ensure that tamper detection measures cannot be bypassed. This may be facilitated by the use of electronic tamper detection equipment. For mobile or portable sources in use, continuous visual surveillance may be the only feasible means of detecting attempted unauthorized removal.

Security objective: Provide immediate assessment of detection.

Security measures: Remote monitoring of CCTV or assessment by operator/ response personnel.

Once an intrusion detection alarm has been triggered, there should be an immediate assessment of the cause of the alarm. Assessment can be performed by operator personnel at the source location, through CCTV or by persons immediately deployed to investigate the cause of the alarm. For mobile or portable sources in use, or in other instances where intrusion detection or tamper detection is provided by continuous visual surveillance by operator personnel, assessment should be performed concurrently with detection by the operator personnel keeping the source under continuous visual surveillance.

Security objective: Provide immediate communication to response personnel.

Security measures: Rapid, dependable means of communication such as phones, cell phones, pagers, radios.

If the assessment confirms that unauthorized access or attempted unauthorized removal has occurred, immediate notification should be made to response personnel by operator personnel with dependable means of communication such as landline telephones, auto-dialers, cellular phones, radios or paging devices.

Security objective: Provide a means to detect loss through verification.

Security measures: Weekly checking through physical checks, tamper detection equipment, etc.

Weekly checking consists of measures to ensure that the sources are present and have not been tampered with. Such measures could include physical checks that the source is in place, verification of seals or other tamper evident devices, and measurements of radiation or other physical phenomena that would provide an assurance that the source is present. For sources in use, verifying that the device is functional may be sufficient.

Delay

Security objective: Provide delay to minimize the likelihood of unauthorized removal.

Security measures: System of two layers of barriers (e.g. walls, cages).

A balanced system of two barriers should separate the source from unauthorized personnel. For sources in use, such measures may include a locked device in a secured area, separating the device from unauthorized personnel. For sources in storage, such measures may include a locked and fixed container or a device holding the source and a locked storage room, separating the container from unauthorized personnel. For mobile or portable sources in use, continuous visual surveillance by operator personnel may substitute for barriers.

Response

Security objective: Provide immediate initiation of response to interrupt unauthorized removal.

Security measures: Equipment and procedures to immediately initiate response.

The operator should establish protocols to ensure immediate deployment of response personnel without delay, in response to an alarm, to interrupt the adversary action. Response may be a directly employed security force, a third party security team, local police, or national gendarmerie. The response should be coordinated with local authorities to mitigate the potential consequences.

Security management

Security objective: Provide access controls to source location that effectively restrict access to authorized persons only.

Security measures: One identification measure.

The purpose of access control is to limit access to the source location to authorized persons, generally by allowing such persons to temporarily disable physical barriers such as locked doors (delay measures) upon verification of the

person's identity and access authorization (in the context of medical exposure, patients do not need to be 'authorized').

The identity and authorization of a person seeking access can be verified by such measures as:

— A PIN to activate a door control reader;
— A badge system which may also activate an electronic reader;
— A badge exchange scheme at an entry control point;
— Biometric features to activate a door control device.

Upon verification of a person's access authorization, the system would allow that person to enter the secured area or source location, e.g. by opening a lock. At least one identification measure should be required, e.g. the use of a swipe card, PIN, computer password, controlled key or visual verification of identity by other authorized personnel. For sources in use, such measures should control access to the area where the source is used. For sources in storage, such measures should control access to the locked room or other location where the source is stored. For mobile or portable sources in use, continuous visual surveillance by operator personnel may substitute for access control.

Security objective: Ensure trustworthiness of authorized individuals.

Security measures: Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information.

An individual's trustworthiness should be assessed through a satisfactory background check before that person is allowed unescorted access to radioactive sources, locations where they are used or stored, or any sensitive, related information. The nature and depth of background checks should be in proportion to the security level of the radioactive source and in accordance with the State's national regulations or as determined by the regulatory body. As a minimum, background checks should involve confirmation of identity and the verification of references to determine the integrity, character and reliability of each person. The process should be periodically reviewed and supported through ongoing attention by supervisors and managers to ensure that personnel at all levels continue to act responsibly and reliably and any concerns, in this context, are made known to the relevant authority.

Security objective: Identify and protect sensitive information.

Security measures: Procedures to identify sensitive information and protect it from unauthorized disclosure.

As well as providing security of radioactive sources, the security system should protect related information, which may include documents, data on computer systems and other media that can be used to identify details of:

— The specific location and inventory of sources;
— The relevant security plan and detailed security arrangements;
— Security systems (e.g. intruder alarms) including performance and installation diagrams;
— Temporary or longer term weaknesses in the security programme;
— Security staffing arrangements and the means of response to events or alarms;
— Planned dates, routes and mode of shipment or transfer of sources;
— Contingency plans and security response measures.

Regulatory guidance should also provide for:

— Control, storage, preparation, identification, marking and transmission of documents or correspondence containing the sensitive information;
— Recommended methods for the destruction of documents containing sensitive information;
— Arrangements covering the declassification and management of documents when they are obsolete or no longer sensitive.

Security objective: Provide a security plan.

Security measures: A security plan which conforms to regulatory requirements and provides for response to increased threat levels.

A security plan should be prepared for each facility by its operator. For examples of content of a security plan, see Appendix II. Security plans may be approved by the regulatory body and reviewed at prescribed intervals during the inspection process to ensure that they reflect the current security system. Security plans may be different for mobile and portable use sources, or for sources stored during periods of use. Most plans are likely to contain sensitive information about protective security arrangements and should therefore be managed accordingly. The security plan should also allow for an efficient and

prompt transition to an enhanced level of security, in the case of an increase in the security threat.

Security objective: Ensure a capability to manage security events covered by security contingency plans.

Security measures: Procedures for responding to security related scenarios.

At each facility contingency plans should be drawn up for a range of events, including:

— A suspected or threatened malicious act;
— A public demonstration which has the potential to threaten the security of sources;
— An intrusion into the secured area by unauthorized person(s). This could range from simple trespass to a determined attack by those seeking to remove or interfere with radioactive sources.

The operator should develop reasonably foreseeable scenarios involving such events and procedures for responding to them. Contingency plans should be shared with appropriate authorities and exercised at regular intervals.

Security objective: Establish security event reporting system.

Security measures: Procedures for timely reporting of security events.

The operator should develop procedures for reporting security events to the regulatory body, first responders, and others as appropriate within a time frame required by the regulatory body commensurate with the security significance of the event. Events to be reported may include:

— Discrepancy in accounting data;
— Suspected or actual theft of a radioactive source;
— Unauthorized intrusion into a facility or source storage area;
— The discovery of a suspected or actual explosive device in or near a facility or store;
— Loss of control over a radioactive source;
— Unauthorized access to or unauthorized use of a source;
— Other malicious acts that threaten authorized activities;
— Suspicious events or sightings which might indicate planning for a sabotage attack, an intrusion or removal of a source;

— Failure or loss of security systems essential for the protection of radioactive sources.

TABLE 8. RECOMMENDED MEASURES FOR SECURITY LEVEL C
(goal: reduce the likelihood of unauthorized removal)

Security function	Security objective	Security measures
Detect	Provide detection of unauthorized removal of the source.	Tamper detection equipment and/or periodic checks by operator personnel.
	Provide immediate assessment of detection.	Assessment by operator / response personnel.
	Provide a means to detect loss through verification.	Monthly checking through physical checks, tamper indicating devices, or other checks to confirm the presence of the source.
Delay	Provide delay to reduce the likelihood of unauthorized removal of a source.	One barrier (e.g. cage, source housing) or under observation by operator personnel.
Response	Implement appropriate action in the event of unauthorized removal of a source.	Procedures for identifying necessary actions in accordance with contingency plans
Security management	Provide access controls to source location that effectively restrict access to authorized persons only.	One identification measure.
	Ensure trustworthiness of authorized individuals.	Appropriate methods for determining the trustworthiness of authorized individuals with unescorted access to radioactive sources and access to sensitive information.
	Identify and protect sensitive information.	Procedures to identify sensitive information and protect it from unauthorized disclosure.
	Provide a security plan.	Documentation of security arrangements and reference procedures.

TABLE 8. RECOMMENDED MEASURES FOR SECURITY LEVEL C
(goal: reduce the likelihood of unauthorized removal) (cont.)

Security function	Security objective	Security measures
	Ensure a capability to manage security events covered by security contingency plans.	Procedures for responding to security related scenarios.
	Establish security event reporting system.	Procedures for timely reporting of security events.

Introduction for Security Level C Measures

The goal of Security Level C is to **reduce the likelihood of unauthorized removal** of radioactive sources. In order to achieve this goal, the following measures are recommended.

Detection

Security objective: Provide detection of unauthorized removal of the source.

Security measures: Tamper detection equipment and/or periodic checks by operator personnel.

Operators should verify that the sources are present. Measures could include physical checks that the source is in place, verification of seals or other tamper indicating devices, and measurements of radiation or other physical phenomena that would provide an assurance that the source is present. For sources in use, verifying that the device is functional may be sufficient.

Security objective: Provide immediate assessment of detection.

Security measures: Assessment by operator or response personnel.

Once tamper detection or a physical check indicates a source may be missing, there should be an immediate assessment of the situation to determine whether an unauthorized removal has actually occurred.

Security objective: Provide a means to detect loss through verification.

Security measures: Monthly checking through physical checks, tamper indicating devices, etc.

Monthly checking consists of measures to ensure that the sources are present and have not been tampered with. Such measures could include physical checks that the source is in place, verification of seals or other tamper indicating devices, and measurements of radiation or other physical phenomena that would provide an assurance that the source is present. For sources in use, verifying that the device is functional may be sufficient.

Delay

Security objective: Provide delay to reduce the likelihood of unauthorized removal of a source.

Security measures: One barrier (e.g. cage, source housing) or under observation by operator personnel.

At least one physical barrier should separate the source from unauthorized personnel. For sources in use, such measures may include the source housing or use of the source in a secured area. For sources in storage, such measures may include a locked and fixed container, a device holding the source or a locked storage room to separate the container from unauthorized personnel. For mobile or portable sources in use, continuous visual surveillance by operator personnel may substitute for the barrier.

Response

Security objective: Implement appropriate action in the event of unauthorized removal of a source.

Security measures: Procedures for identifying necessary actions in accordance with contingency plans.

Regulatory procedures should ensure that any suspected unauthorized removal or loss of a source is assessed and, if confirmed, reported to the appropriate authority without delay. This should be followed by an effort to locate and recover the source and investigate the circumstances leading to the event.

Security management

Security objective: Provide access controls to source location that effectively restrict access to authorized persons only.

Security measures: One identification measure.

Access control is intended to limit access to the source location to authorized persons, generally by allowing such persons to temporarily disable physical barriers such as locked doors (delay measures) upon verification of the person's identity and access authorization. (In the context of medical exposure, patients do not need to be "authorized.")

The identity and authorization of a person seeking access can be verified by such measures as:

— A PIN to activate a door control reader;
— A badge system which may also activate an electronic reader;
— A badge exchange scheme at an entry control point;
— Biometric features to activate a door control device.

Upon verification of a person's access authorization, the system would allow that person to enter the secured area or source location, e.g. by opening a lock. At least one identification measure should be required, e.g. the use of a swipe card, PIN, computer password, controlled key or visual verification of identity by other authorized personnel. For sources in use, such measures should control access to the area where the source is used. For sources in storage, such measures should control access to the locked room or other location where the source is stored. For mobile or portable sources in use, continuous visual surveillance by operator personnel may substitute for access control.

Security objective: Ensure trustworthiness of authorized individuals.

Security measures: Appropriate methods for determining the trustworthiness of authorized individuals with unescorted access to radioactive sources and access to sensitive information.

An individual's trustworthiness should be assessed through a satisfactory background check before that person is allowed unescorted access to radioactive sources, locations where they are used or stored, or any sensitive,

related information. The nature and depth of background checks should be in proportion to the security level of the source and in accordance with the State's national standards or as determined by the regulatory body.

Security objective: Identify and protect sensitive information.

Security measures: Procedures to identify sensitive information and protect it from unauthorized disclosure.

Regulatory provisions should ensure that the operator assesses whether those individuals with access to security information or radioactive sources are reliable. Unless determined to be trustworthy, they should not be granted unescorted access.

Security objective: Provide a security plan.

Security measures: Documentation of security arrangements and reference procedures.

Security arrangements and reference procedures should be adopted in the form of a security plan. For examples of the content of a security plan, see Appendix II.

Security objective: Ensure a capability to manage security events covered by security contingency plans.

Security measures: Procedures for responding to security related scenarios.

The security statement should include procedures for investigating and reporting any unauthorized access to or removal of a source.

Security objective: Establish a security event reporting system.

Security measures: Procedures for timely reporting of security events.

The operator should develop procedures for reporting of security events to the regulatory body, first responders, and others as appropriate within a time frame required by the regulatory body commensurate with the security significance of the event. Events to be reported may include:

— Discrepancy in accounting data;

— Suspected or actual theft of a radioactive source;
— Unauthorized intrusion into a facility or source storage area;
— Discovery of a suspected or actual explosive device in or near a facility or store;
— Loss of control over a radioactive source;
— Unauthorized access to or unauthorized use of a source;
— Other malicious acts that threaten authorized activities;
— Suspicious events or sightings which might indicate planning for a sabotage attack, an intrusion or removal of a source;
— Failure or loss of security systems that are essential to the protection of radioactive sources.

4.3.2. Performance based approach

The regulatory body may choose to specify the use of a performance based approach by which operators meet applicable security objectives. Generally, a State's choice of approach will depend on the availability of security expertise to the regulatory body and the operator. A performance based approach would function most effectively where operators have professional advisers and expertise to design and implement the necessary measures and have demonstrated a sustained record of consistency and compliance. The regulatory body should ensure that the approved measures are clearly documented, e.g. within a security plan, and assessed at appropriate intervals.

For the performance based approach, a State will need to use the national threat assessment, and may also choose to develop a DBT where applicable. The regulatory body should further specify a security objective for the classes of sources to which the performance-based approach applies. Generally, such security objectives should be stated in terms of required system effectiveness, as described in Section 3.

A security system that meets applicable security objectives should then be developed by conducting a VA against the applicable DBT or assessed threat. Depending upon the circumstances, this assessment may be performed by the regulatory body or by the operator, using the approach described in Section 3 or another methodology, as determined by the regulatory body. The results of the VA or other methodology would also be used to demonstrate that the resulting security system does, in fact, meet the applicable security objectives.

The set of security measures developed by applying the performance based approach would not necessarily correspond to the security measures for the particular source that would be recommended by the prescriptive approach listed in Tables 6–8. While measures addressing the security functions of

detection, *delay*, and *response* from Table 2 would be included, the particular combination of measures may vary in light of the situation specific analysis conducted in the VA. Application of the performance based approach generally leads to a more tailored and cost effective set of security measures than is possible using the prescriptive approach. The performance based approach does not lend itself to a statistical analysis of *deterrence* or *security management* although these functions are an integral part of the programme. Accordingly, the performance based approach should also include a requirement for deterrence and security management measures applicable to the security level of the source or sources involved, as described in the material on the prescriptive approach. The performance based approach should consider the systematic interaction of detection, delay and response in determining overall system effectiveness against the assessed threat.

System effectiveness is the key measure of the performance based approach. In order to design a security system using the performance based approach, an assumption is made that any deterrence measures will fail and that a malicious act is attempted. The security system should then be designed to achieve the required level of system effectiveness in preventing the malicious act assumed to occur in light of the assessed threat.

4.3.3. Combined approach

Many States may wish to combine aspects of both the prescriptive- and performance based approaches in order to apply security measures that meet the security objectives stated above. For example, a State could use the prescriptive approach for radioactive sources with lower potential consequences of malicious use, but apply the performance based approach to the most dangerous sources. For those most dangerous sources, the State would conduct a national threat assessment and develop a DBT. The operator would then be responsible for applying the appropriate security measures to meet a set of security objectives defined in terms of the security functions of *deterrence*, *detection*, *delay*, *response* and *security management*.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Code of Conduct on the Safety and Security of Radioactive Sources, IAEA/CODEOC/2004, IAEA, Vienna (2004).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources (Interim Guidance for Comment), IAEA-TECDOC-1355, IAEA, Vienna (2003).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Categorization of Radioactive Sources, IAEA Safety Standards Series No. RS-G-1.9, IAEA, Vienna (2005).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Radiation Generators, IAEA Safety Standards Series No. RS-G-1.10, IAEA, Vienna (2007).

[5] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, Safety Series No. 115, IAEA, Vienna (1996).

[6] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles IAEA Safety Standards Series No SF-1, IAEA, Vienna (2006).

[7] International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations, New York (2005).

[8] Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (1980); CPPNM Amendment, GOV/INF/2005/10–GC(49)/INF/6, IAEA, Vienna (2005).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency IAEA Safety Standards Series No. GS-R-2, IAEA, Vienna (2002).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Remediation of Areas Contaminated by Past Activities and Accidents Safety Requirement, IAEA Safety Standards Series No. WS-R-3, IAEA, Vienna (2003).

[11] INTERNATIONAL COMMISION ON RADIOLOGICAL PROTECTION, Protecting People against Radiation Exposure in the Event of A Radiological Attack Publication 96, Pergamon Press, Oxford (2005).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No. 9, IAEA, Vienna (2008).
[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).
[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).
[15] INTERNATIONAL ATOMIC ENERGY AGENCY Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Legal and Governmental Infrastructure for Nuclear, Radiation, Radioactive Waste and Transport, IAEA Safety Standards Series No. GS-R-1, IAEA, Vienna (2000).
[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Dangerous Quantities of Radioactive Material (EPR-D-Values), IAEA, Vienna (2006).
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, IAEA, Vienna (2007), http://www-ns.iaea.org/standards/safety-glossary.html.
[19] The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev.4 (Corrected), IAEA, Vienna (1999).

DEFINITIONS

authorization. A permission granted in a document by a regulatory body to a person who has submitted an application to manage a radioactive source. The authorization can take the form of a registration, a licence or alternative effective legal control measures which achieve the objectives of the Code of Conduct (adopted from Ref. [1]).

design basis threat. A comprehensive description of the motivations, intentions, and capabilities of potential adversaries against which protection systems are designed and evaluated (adapted from Ref. [13]).

disused source. A radioactive source which is no longer used, and is not intended to be used, in facilities and activities for which authorization has been granted (adopted from Ref. [18]).

malicious act. A wrongful act or activity intentionally done or engaged in without legal justification or excuse (e.g. smuggling) or an act or activity intended to cause death or physical injury to any person, material damage to any person (e.g. theft) or damage to property or to the environment (adopted from GOV/2002/10).

operator. Any organization or person applying for authorization or authorized and/or responsible for nuclear, radiation, radioactive waste, or transport safety when undertaking activities or in relation to any nuclear facilities or sources of ionizing radiation. This includes private individuals, governmental bodies, consignors or carriers, licensees, hospitals, self-employed persons, etc. (adopted from Ref. [18]).

radioactive source. Radioactive material that is permanently sealed in a capsule or closely bonded, in a solid form and which is not exempt from regulatory control. It also means any radioactive material released if the radioactive source is leaking or broken, but does not mean material encapsulated for disposal, or nuclear material within the nuclear fuel cycles of research and power reactors (adopted from Ref. [1]).

regulatory body. An entity or organization or a system of entities or organizations designated by the government of a State as having legal authority for exercising regulatory control with respect to radioactive sources, including issuing authorizations, and thereby regulating one or more aspects of the safety or security of radioactive sources (adopted from Ref. [1]).

sabotage. Deliberate damage; sabotage in this context means deliberate damage to a radioactive source in use, storage or transport or to an associated facility. A deliberate act directed against a radioactive source in use, storage or transport could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive material (adapted from Ref. [19]).

(nuclear) security. The prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities (adopted from Ref. [12]).

security culture. The characteristics and attitudes in organizations and of individuals which establish that security issues receive the attention warranted by their significance (adopted from Ref. [1]).

security contingency plan. A part of the security plan or a stand-alone document that identifies reasonably foreseeable security events, provides initial planned actions, (including alerting appropriate authorities) and assigns responsibilities to appropriate operator personnel and response personnel.

security plan. A document — prepared by the operator and possibly required to be reviewed by the regulatory body — that presents a detailed description of the security arrangements in place at a facility.

storage. The holding of radioactive sources in a facility that provides for their containment with the intention of retrieval (adopted from Ref. [1]).

threat assessment. An analysis that documents the credible motivations, intentions and capabilities of potential adversaries that could cause undesirable consequences with regard to radioactive material in use or storage and its associated facilities (adopted from Ref. [12]).

unauthorized removal. The theft or other unlawful taking of radioactive sources (adapted from Ref. [19]).

vulnerability assessment (VA). A process which evaluates and documents the features and effectiveness of the overall security system at a particular facility.

This report provides guidance and recommended measures for the prevention, detection and response to malicious acts involving radioactive sources. It is intended to help prevent the loss of control of such sources. It also recommends that security measures be applied to radioactive sources in manufacture, use and short term or long term storage. This Implementing Guide recommends that security measures be applied on a graded basis, taking into account the current evaluation of the threat, the relative attractiveness of the source, and the potential consequences resulting from malicious use. The requisite level of security is achieved through a combination of deterrence, detection, delay, response and security management.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–102609–5
ISSN 1816–9317