Aplicación operador	Requisito		Orientaciones para la implementación	Evidencias (*)
Todos los operadores: • Exportador • Importador • Depósito • Zona franca • Usuario de ZF • Transportista • Despachante de aduana • Agente de carga • Terminal de carga aérea • Operador portuario • Agencia marítima	**REQUISITO OEC Nº 1 Constitución legal, antigüedad y cumplimiento de normativa**	La organización debe: 1) Estar legalmente constituida. 2) Tener una antigüedad mínima de acuerdo a lo establecido en el Decreto N° 210/015. 3) Identificar los requisitos legales y reglamentarios que le correspondan, tanto para operar en Uruguay, como en los países en los que tiene negocios. 4) Identificar todas las autorizaciones asociadas a requisitos del numeral anterior y contar con los respectivos documentos, vigentes y en condiciones de hacerlos disponibles para su comprobación por parte de la DNA.	Con este requisito se pretende que la organización evite que sus actividades se vean impedidas por incumplimientos de requisitos legales de constitución u operación, en el entendido de que la interrupción de la operación aumenta los riesgos de ilícitos. La DNA analizará: a) Los documentos constitutivos de la organización que además permitan verificar su antigüedad. b) La existencia de un listado actualizado de los requisitos legales y reglamentarios requeridos, y de los documentos correspondientes, fechas de validez, un responsable de verificar periódicamente su cumplimiento, vigencia, y la fuente de información utilizada para la verificación.	• Documentos constitutivos - Certificado notarial acreditando constitución, plazo, objeto, representación, vigencia, inscripción registral y publicaciones legales. • Listado de habilitaciones y/o autorizaciones para operar.
Todos los operadores	**REQUISITO OEC Nº 2 Solvencia Financiera**	La organización debe: 1) Poseer solvencia financiera. 2) No encontrarse en procesos de concurso. 3) No poseer embargos judiciales ni estar sancionada mediante sentencia o resolución condenatoria en firme por falta de pago. 4) Cumplir con las normas contables de aplicación obligatoria de acuerdo a lo establecido por la Dirección General Impositiva en cuanto a la preparación y presentación de estados contables. 5) Presentar los estados contables de los últimos tres años a la fecha de la Solicitud OEC. 6) Cuando no existan calificaciones de riesgo crediticio publicadas por el Banco Central del Uruguay (BCU), presentar al menos cuatro referencias comerciales que certifiquen que operó internacionalmente sin inconvenientes financieros, cumpliendo regularmente con sus obligaciones de pago durante los tres últimos años.	Los estados financieros sirven de base objetiva para determinar la situación financiera de una empresa. A estos efectos, se tomarán en cuenta los ratios: a) Índice de liquidez: i. Razón Corriente ii. Prueba ácida menor iii. Prueba ácida mayor b) Índice de endeudamiento i. Leverage o índice de endeudamiento c) Y las calificaciones de riesgo crediticio publicadas por el BCU cuando estas existan, considerándose aceptables cuando las mismas estén comprendidas en el rango 1A a 3 inclusive.	• Estados contables auditados o informe de revisión limitada, según corresponda. • Informe de la Central de riesgo crediticio del BCU. •Referencias comerciales, en caso que corresponda.

Todos los operadores	**REQUISITO OEC Nº 3** **Historial de cumplimiento aduanero y tributario**	La organización debe: 1) Tener un historial de cumplimiento aduanero y tributario satisfactorio de acuerdo a los criterios establecidos por la Dirección Nacional de Aduanas. 2) Presentar declaración jurada detallando antecedentes penales, causas en proceso o cerradas de los últimos tres años que vinculen a la empresa, sus propietarios o directores con delitos o infracciones aduaneras, tributarias o penales relacionadas a narcotráfico, terrorismo, contrabando, piratería, tráfico de armas y/o personas, delitos relacionados con el lavado de activos y delitos precedentes de éste, u otras vinculadas con la seguridad del comercio exterior. En caso de no existir ninguna causa en proceso o cerrada, explicitarlo en la declaración jurada. La existencia de sanciones o juicios no implica necesariamente que la misma no pueda participar en el Programa OEC. Se analizará caso a caso.	Para valorar este requisito se evaluarán: a) Las infracciones cometidas por los operadores en los últimos tres años previos a la solicitud de ingreso al Programa OEC, o a la renovación de su certificación. A tales efectos se utilizará como herramienta el software Historial de cumplimiento. El tipo y cantidad de infracciones es evaluado directamente por la Dirección Nacional de Aduanas. b) Las declaraciones juradas, los certificados de antecedentes judiciales y los informes que se solicitarán a distintas oficinas de la Dirección Nacional de Aduanas.	• Declaración jurada OEC.RG.30. • Certificado de antecedentes judiciales de sus propietarios o directores.
Todos los operadores	**REQUISITO OEC Nº 4** **Sistema de Gestión de la Seguridad (SGS)**	La organización debe: 1) Documentar, implementar, mantener y mejorar en forma continua un SGS que le resulte eficaz para identificar, tratar, controlar y minimizar las consecuencias de los riesgos de seguridad de su cadena de suministro internacional. 2) Diseñar, implementar y respaldar el SGS en base a un componente de revisión documentado que debe ser actualizado, según sea necesario, en función de los cambios pertinentes en las operaciones y el nivel de riesgo de una organización.		•Documentación del SGS que da cumplimiento a todos los requisitos.
Todos los operadores	**4.1** **Política de seguridad**	La organización debe: 1) Contar con una Política de seguridad documentada, firmada por la dirección, que promueva una cultura en seguridad de la cadena de suministro. 2) Manifestar en la Política de seguridad el compromiso que asume la organización de tomar las medidas a su alcance para evitar verse involucrada en actos ilícitos en su cadena de suministro internacional, y su compromiso de cumplir la normativa nacional e internacional vigente. 3) Hacer referencia explícita en su Política de seguridad a las actividades ilícitas asociadas al comercio internacional como ser narcotráfico, contrabando, terrorismo, tráfico de productos falsificados, tráfico de armas, entre otros. 4) Transmitir la Política de seguridad a todos los funcionarios de la organización, debiéndose evaluar su entendimiento. 5) Exhibir la Política de seguridad en las instalaciones de la organización y en su sitio web para su comunicación, promoción y puesta en práctica. Asimismo, debe ser entregada y/o enviada a sus socios comerciales para su conocimiento.	La política de seguridad: a) Debe explicitar las actividades asociadas al comercio exterior para diferenciar claramente el objeto del SGS en el marco del Programa OEC, respecto de otros sistemas de gestión relacionados con calidad, seguridad laboral, medioambiental u otros. b) Ser comunicada a sus empleados en instancias como la inducción a nuevos empleados, y en capacitaciones específicas, guardando los registros correspondientes. c) Ser comunicada a sus socios comerciales, clientes y proveedores, dejando los registros correspondientes. Dicha comunicación debe ser realizada también toda vez que se incorpore un nuevo cliente y proveedor. d) Ser difundida interna y externamente cada vez que se realice una modificación o actualización de la misma.	• Política de seguridad. • Registros de difusión a la interna de la organización. • Evaluación del entendimiento de la política. • Registro de difusión a los socios comerciales (clientes y proveedores).

• Exportador • Importador • Zona franca y Usuario de ZF (Según corresponda)	**4.2** **Política contra el trabajo forzoso, trabajo infantil o encarcelado**	La organización debe: 1) Contar con una política o declaración de cumplimiento social documentada, que vele por trabajar con socios comerciales cuyos bienes no sean extraídos, producidos o fabricados, total o parcialmente, con formas de trabajo prohibidas, tales como trabajo forzoso, trabajo infantil, o encarcelado. 2) Asegurar que la política o declaración de cumplimiento social establezca lo que se espera en relación con los derechos humanos, de su personal, sus socios y otras partes directamente vinculadas con sus operaciones, productos o servicios. 3) Dar a conocer públicamente sus responsabilidades, compromisos y expectativas en este sentido.	La política o declaración de cumplimiento social: a) Debe describir cómo la organización toma recaudos para que los bienes que importa no se produzcan o fabriquen, total o parcialmente con formas de trabajo prohibidas (forzadas, trabajo infantil, encarcelado). b) Puede estar incluida dentro de la Política de seguridad, en un código de conducta, en la sección de compromiso de Responsabilidad Social Empresarial (RSE), o bien establecerse en un documento aparte. c) Su difusión debe ser registrada.	• Política o declaración contra el trabajo forzoso, trabajo infantil o encarcelado. •Registros de difusión.

Todos los operadores	**4.3 PLANIFICACIÓN DE LA SEGURIDAD** **4.3.1** **Análisis de Riesgo**	La organización debe: 1) Contar con un SGS planificado en base a un análisis de riesgo. 2) Establecer un procedimiento documentado para el análisis de riesgo que incluya: a. la metodología para la evaluación de los riesgos; b. las amenazas externas vinculadas a actividades ilícitas como terrorismo, narcotráfico, crimen organizado en las cadenas de suministro de las que participa; c. las vulnerabilidades internas de la organización, y externas vinculadas a sus socios comerciales directos e indirectos. 3) Realizar y documentar una evaluación de riesgos que permita: a. identificar los riesgos de las cadenas de suministro en las que participa en general, y los riesgos a los que están expuestas sus operaciones en particular; b. determinar la probabilidad de ocurrencia, la importancia de las consecuencias de cada riesgo identificado y la probabilidad de detección; c. determinar el grado de control o la incidencia sobre cada riesgo identificado; d. establecer medidas de prevención y acciones de control adecuadas a cada riesgo analizado, así como la evaluación de su eficacia conformando un programa de seguridad con plazos, recursos y responsables para su ejecución. 4) Incluir en la evaluación de riesgos los requisitos de seguridad OEC que le apliquen según su rol en la cadena de suministro, debiendo comprender todos los componentes del SGS (instalaciones, equipos, mercaderías, procesos, personas, información, socios comerciales, etc.) que la organización defina como críticos en materia de seguridad, de acuerdo a la naturaleza y a la escala del propio modelo empresarial. 5) Documentar o mapear en la evaluación de riesgos internacionales el flujo de la gestión documental y el movimiento de la carga a lo largo de su o sus cadenas de suministro, desde el punto de origen hasta el punto de destino. 6) Mapear cómo la carga entra y sale de las instalaciones del transportista y/o centros de carga, y observar si la carga permanece detenida o "en reposo" en una de estas ubicaciones durante un período de tiempo prolongado. 7) Incluir en el mapeo a todos los socios comerciales involucrados directa e indirectamente, tanto en la gestión documental como en el movimiento de la carga de exportación, importación y/o tránsito. 8) Revisar el análisis de riesgo anualmente o con mayor frecuencia según lo requieran los factores de riesgo, cuando se produzca una infracción o un incidente de seguridad.	La importancia de un enfoque basado en riesgo es garantizar que las medidas de seguridad para prevenir o mitigar las interrupciones de la cadena de suministro sean proporcionales a los riesgos identificados. El análisis de riesgos requiere que los operadores efectúen un análisis de acuerdo a su rol en la cadena de suministro, las vulnerabilidades internas en cuanto al cumplimiento de los requisitos, y la aplicación de los procedimientos de seguridad. Adicionalmente, se requiere evaluar las vulnerabilidades asociadas con los distintos actores de la cadena de suministro internacional. Los operadores deben evaluar todas las amenazas relevantes para sus cadenas de suministro en función de indicadores tales como la complejidad de la cadena de suministro en sí (número de socios comerciales a lo largo de la cadena de suministro/tiempo que la carga está en reposo), presencia de organizaciones terroristas o traficantes de drogas en los países de origen, destino o tránsito, historial de interrupciones de carga (como evidencia de manipulación, robo de carga o introducción de contrabando). Las amenazas geográficas (punto de origen/destino y/o tránsito) y la vulnerabilidad del cumplimiento de los requisitos de seguridad OEC/OEA de los socios comerciales son factores críticos. El mapeo de la cadena de suministro es el método de identificación de todos los participantes o socios involucrados directa e indirectamente en la cadena de suministro internacional (comprende procesos tales como exportación, importación, movimiento de mercadería, gestión documental) desde el punto de origen hasta el centro de distribución, es decir, desde el principio hasta el final de la cadena de suministro. Las circunstancias pueden requerir que se revise la evaluación de riesgo con mayor frecuencia que una vez al año, incluyendo un mayor nivel de amenaza de un país específico, períodos de intensificación de alertas, luego de un incidente o falla de la seguridad, cambios en los socios comerciales, o cambios en la participación o estructura empresarial, como fusiones y adquisiciones, entre otros. Para aquellas organizaciones que participan en varias cadenas de suministro y/o que cuentan con muchos actores involucrados es recomendable iniciar el análisis identificando sus cadenas de suministro de “Alto Riesgo”, y posteriormente avanzar en el análisis de las cadenas de suministro que implican un número limitado de socios comerciales o de socios relacionados.	• Procedimiento de análisis de riesgo. •Matriz de riesgo. • Registro de evaluación de las cadenas de suministro y evaluación de riesgos internacionales.

Todos los operadores	**4.3.2 Objetivos e indicadores**	La organización debe: 1) Definir objetivos de seguridad alineados a la política de seguridad y a la planificación de la seguridad (análisis de riesgo). Estos deben ser concretos, cuantificables, establecer plazos, metas a alcanzar y responsable, y deben estar en conocimiento de todo el personal. 2) Definir e implementar para cada área de la misma, indicadores de seguridad (definidos a partir de los objetivos de seguridad) y una metodología para su medición y seguimiento. 3) Revisar y actualizar los objetivos e indicadores de seguridad periódicamente, para asegurar su continua vigencia y pertinencia, su análisis debe permitir identificar las acciones de mejora necesarias para mantener y mejorar la eficacia de su SGS.	Los resultados del análisis de riesgo son una fuente de información para definir objetivos e indicadores. Para aquellos riesgos definidos como críticos, se deben definir indicadores que permitan monitorear la exposición de la empresa respecto de esos riesgos. Por ejemplo, la cantidad y tipo de errores detectados en los controles de documentación representan una medida directa del riesgo que tiene la empresa de que un embarque tenga problemas; la rotación del personal y el ausentismo son medidas indirectas del ambiente laboral, y por lo tanto del riesgo de que algún empleado tome alguna acción que pueda perjudicar a la empresa.	•Objetivos e indicadores anuales, planificación, seguimiento y cierre.
Todos los operadores	**4.3.3 Preparación y respuesta ante emergencias - Gestión de crisis**	La organización debe: 1) Establecer un procedimiento con protocolos de actuación y/o planes de contingencia y de continuidad del negocio, documentados, para actuar frente a las situaciones de emergencia identificadas en el análisis de riesgo, de modo de minimizar su impacto sobre la seguridad de las operaciones de comercio exterior y de la organización en su conjunto. 2) Verificar la vigencia, aplicabilidad y eficacia de los protocolos y/o planes de contingencia y de continuidad del negocio, en oportunidad de la evaluación de la adecuación del SGS al análisis de riesgo (una vez al año o cuando se produzca un incidente de seguridad). 3) Planificar, realizar y documentar simulacros en los que se pongan a prueba los protocolos de actuación incluidos en el procedimiento de respuesta ante emergencias.	La preparación y respuesta ante emergencias resulta una herramienta fundamental para evaluar la eficacia de los procedimientos establecidos. Dado que la mayoría de las medidas adoptadas responden a riesgos de baja probabilidad de ocurrencia, pero de alto impacto en caso de que sucedan, la forma de evaluar la eficacia de estas medidas es realizando simulacros. Además de las medidas preventivas para mitigar los riesgos que surgen en la etapa de planificación, la empresa debe prepararse para el caso de que el evento evaluado como crítico ocurra. La organización debe: a) definir planes de contingencia y/o protocolos para actuar ante una emergencia, b) capacitar al personal, c) definir un plan de simulacros, y d) evaluar los resultados. El registro de simulacros deberá contar con fecha de realización, responsables, una descripción del simulacro, evaluación, resultados y conclusiones, y acciones a tomar.	• Procedimiento de preparación y respuesta ante emergencias con protocolos definidos para las situaciones de emergencia identificadas en el análisis de riesgo y de continuidad del negocio. • Registro de la planificación de simulacros. • Registro de simulacros.

Todos los operadores	**4.4 IMPLEMENTACIÓN DE LA SEGURIDAD** **4.4.1 Documentación del sistema de gestión**	La organización debe: 1) Contar con la documentación necesaria para resguardar, fortalecer y mejorar el conocimiento que la organización tiene sobre su propio SGS. Para cumplir eficazmente estos cometidos, la documentación debe ser clara, precisa y concisa. El diseño de la documentación debe centrarse en la eficiencia y ser aplicable a la organización. 2) Asegurar que la estructura documental del SGS contenga al menos: a. Manual de seguridad que incluya entre otros elementos el alcance, la política de seguridad, el modelo de negocio de la organización y sus procesos, la descripción de los elementos del SGS, y referencias a los documentos relevantes que dan cumplimiento a los requisitos OEC. b. Procedimientos que describan cómo se realizan las actividades para dar cumplimiento a los requisitos OEC, alcance, responsabilidades, registros resultantes de las actividades descritas y otros documentos. c. Instructivos que describan de manera clara y precisa los pasos a seguir para realizar correctamente una actividad o trabajo específico, alcance, responsabilidades, registros resultantes de las actividades descritas y otros documentos que deban ser referenciados para dar cumplimiento a los requisitos OEC. d. Documentos y registros relativos a la planificación, implementación, control y verificación de la seguridad, revisión por la dirección y mejora continua del SGS.		•Manual SGS. •Procedimientos. •Instructivos. •Registros y evidencias de la implementación.
Todos los operadores	**4.4.2 Control de documentos del sistema de gestión**	La organización debe: 1) Establecer un procedimiento documentado para elaborar y controlar la documentación del SGS (de origen interno y externo) y asegurar que: a. sea elaborada, revisada y aprobada por personal autorizado; b. se almacene adecuadamente y permanezca protegida contra daños, deterioro, pérdida o uso indebido; c. sea revisada periódicamente, como mínimo una vez al año, y actualizada cuando sea necesario; d. sea de fácil acceso y esté disponible oportunamente para cada persona de la organización, en la medida y con el grado de detalle que sus responsabilidades lo requieran; e. las versiones vigentes de los documentos estén disponibles en todos los sitios en los que se los requiera para el eficaz funcionamiento del SGS; f. las versiones obsoletas sean fácilmente identificables y evitar el uso de las mismas. 2) Determinar el grado de confidencialidad de la documentación del SGS y comunicar su contenido apropiadamente, tanto en la interna de la organización como a los socios comerciales (según el grado de responsabilidad correspondiente a cada involucrado).	El control de documentos tiene como propósito hacer cumplir los procesos y prácticas para la creación, revisión, modificación, emisión, distribución y accesibilidad de los documentos. Permite asegurar que la documentación disponible dentro de la organización contenga información actualizada, confiable, verificada y aprobada formalmente. Las áreas operativas deben revisar la documentación a efectos de su compatibilidad con la actividad y operativa diaria. Asimismo, se debe asegurar que los documentos de origen externo sean identificados, y su distribución sea controlada. La organización debe identificar el grado de confidencialidad de los documentos y definir quién puede tener acceso a los mismos. Si se realizan cambios en un documento debe existir un mecanismo para notificar a todas las partes interesadas para evitar el uso de una versión desactualizada.	• Procedimiento de elaboración y control de documentos. • Listado maestro de documentos. • Registro que contenga niveles de confidencialidad.

Todos los operadores	**4.4.3 Responsabilidad y autoridad**	La organización debe: 1) Contar con un organigrama en el que se represente la estructura interna de la misma, reflejando las autoridades y relaciones jerárquicas. 2) Tener claramente establecidas las responsabilidades de todos sus integrantes, autoridades y personal, en relación a la seguridad de la cadena de suministro en sus procedimientos y/o perfiles de cargo. 3) Asegurar que la alta dirección se involucre activamente con la mejora continua de la seguridad de la organización, demostrando que cumple sus compromisos como máximo responsable por la seguridad de las cadenas de suministro internacional en las que participa la organización. Consecuentemente, debe asignar los recursos necesarios para el correcto funcionamiento del SGS en su conjunto. 4) Designar a una persona responsable del SGS para su diseño, implementación, documentación, revisión, mantenimiento y mejora. Dicha persona debe ser parte de la organización. 5) Asegurar que la persona responsable del SGS tenga conocimiento de los requisitos y de todo el Programa OEC, y tenga las potestades necesarias para garantizar el cumplimiento de todos los requisitos de seguridad, así como la puesta en práctica de medidas preventivas y correctivas que entienda pertinentes a tales efectos. 6) Designar a su Representante OEC quien será el nexo en todas las instancias vinculadas al proceso de certificación, mantenimiento o renovación, así como en las comunicaciones con la DNA vinculadas a cambios en su SGS o incidentes de seguridad en las cadenas de suministro en las que participa la organización. Dicha persona debe ser parte de la organización. Ambas designaciones pueden coincidir en la misma persona, debiendo informar al Departamento OEC apenas se produzca cualquier cambio en relación a las mismas.	Las responsabilidades de todo el personal en relación a la seguridad de la cadena de suministro deben estar claramente definidas a los efectos de establecer una estructura más sostenible y enfatizar que la seguridad de la cadena de suministro es responsabilidad de todos. La persona designada como responsable de implementar y mantener el SGS debe: a) ser parte de la organización, b) tener un amplio conocimiento de los requisitos de seguridad, c) conocer en profundidad las prácticas y los procedimientos de la organización, y d) debe garantizar el cumplimiento de los requisitos. e) Informar periódicamente y poner en conocimiento a la dirección y al equipo interdisciplinario sobre los resultados del funcionamiento del SGS, por ejemplo, cuando se realicen simulacros debe coordinar la realización de los mismos y comunicar los resultados obtenidos.	• Organigrama • Perfiles de cargo / procedimientos con descripción de tareas donde se establezcan las responsabilidades en relación al SGS. •Formulario de designación del representante OEC y encargado del SGS OEC.RG.04.
Todos los operadores		7) Conformar un equipo interdisciplinario integrado por los dueños de los procesos más relevantes. 8) Establecer que el responsable del SGS o el equipo interdisciplinario, según corresponda, deben proporcionar a la dirección actualizaciones periódicas sobre incidentes de seguridad, resultados de simulacros y de auditorías, evaluaciones y ejercicios realizados al SGS.	Se debe conformar un equipo interdisciplinario que involucre a los responsables de los procesos más importantes como, por ejemplo, recursos humanos, tecnología de la información, operativos, planificación, comercial, etc. a los efectos de que todos estén involucrados y puedan intercambiar información y conocimiento de los aspectos de seguridad más relevantes para la organización.	

Todos los operadores	**4.4.4 Toma de Conciencia y competencias**	La organización debe: 1) Establecer un programa de concientización y capacitación en seguridad de la cadena de suministro con el objetivo de lograr que todo el personal tome conciencia de: a) sus responsabilidades en materia de seguridad; b) los riesgos de contrabando, narcotráfico, terrorismo, falsificaciones y otras actividades ilícitas asociadas al comercio internacional; c) cómo reconocer las vulnerabilidades de la seguridad de las instalaciones, medios de transporte y carga en cada punto de la cadena de suministro que puedan ser utilizadas por grupos delictivos o implicar conspiraciones internas. 2) Diseñar y actualizar el programa de capacitación, por lo menos una vez al año, de acuerdo a los riesgos identificados y evaluar los resultados de su ejecución. El programa debe ser completo y cubrir todos los requisitos de seguridad OEC. 3) Proporcionar capacitación en seguridad a los empleados, según se requiera, en función de sus responsabilidades, tareas y puesto de trabajo, de manera regular. El personal en puestos sensibles debe recibir capacitación especializada adicional, orientada a las responsabilidades que tiene el puesto. 4) Brindar capacitación a los empleados recién contratados como parte de su inducción sobre el SGS, los requisitos de seguridad y sus responsabilidades. 5) Realizar periódicamente una actualización de las capacitaciones según sea necesario, después de un incidente de seguridad, y/o cuando haya cambios en los procedimientos de la organización. 6) Brindar capacitación especializada anualmente en los siguientes temas, de acuerdo al puesto y las responsabilidades asignadas: a) Indicadores de alerta de lavado de dinero basado en el comercio y financiamiento del terrorismo. b) Prevención de la contaminación visible por plagas. La capacitación debe abarcar las medidas de prevención de plagas, los requisitos reglamentarios aplicables a los materiales de embalaje de madera y la identificación de la madera infestada. c) Inspección de medios de transporte vacíos y de los ITI en materia de seguridad y con fines agrícolas, debiendo incluir señales de compartimentos ocultos, ejemplos de contrabando oculto en compartimentos naturales y señales de contaminación por plagas. d) Seguridad de los precintos y su verificación. e) Procedimientos con los protocolos de actuación y/o planes de contingencia ante emergencias y continuidad del negocio. f) Procedimientos a seguir en caso de detección de mercadería sospechosa durante una inspección de la unidad, o en caso de que se produzca un incidente de seguridad durante el transporte. g) Políticas y procedimientos de ciberseguridad de la empresa, debiendo incluir la necesidad de que los empleados protejan las contraseñas y el acceso a las computadoras.	La temática de las capacitaciones se ajustará en función del modelo de negocio y el contacto con la carga. Uno de los aspectos clave del programa de seguridad de la organización es la capacitación. La capacitación en materia de seguridad garantiza que los empleados reciban la información necesaria para identificar, prevenir y responder a las amenazas e infracciones a la seguridad. Los empleados que son conscientes de los riesgos y amenazas de seguridad, del papel de la organización en la cadena de suministro, y que entienden el porqué de las medidas de seguridad tienen más probabilidades de adherirse a las mismas. Los empleados deben recibir capacitación sobre seguridad en la cadena de suministro de forma periódica, al menos una vez al año. Los empleados recién contratados deben recibir capacitación en seguridad de la cadena de suministro como parte de su inducción laboral. El programa de capacitación debe ser completo y abarcar todos los requisitos de seguridad del Programa OEC. La organización debe conservar registros de las capacitaciones brindadas a los empleados, y disponer de medidas para verificar que la capacitación impartida cumpla con todos los objetivos planteados. Comprender la capacitación y ser capaz de utilizarla en el propio puesto (en particular por los empleados con puestos sensibles) es de vital importancia. Las verificaciones, los simulacros o las auditorías periódicas de los procedimientos, etc., son algunas de las medidas que la empresa puede aplicar para determinar la eficacia de la capacitación.	• Plan de capacitación (inducción, capacitaciones periódicas, cartelería, charlas, eventos). •Registros de cada capacitación.

		7) Capacitación en operación, mantenimiento y administración de los sistemas de tecnología de seguridad. 8) Capacitar al personal sobre cómo informar incidentes de seguridad y actividades sospechosas que puedan implicar conspiraciones internas, contaminación o alteración de la carga o de la documentación. 9) Conservar evidencia de las capacitaciones debiendo contener el tema, la fecha de realización y la lista de participantes (nombres de los asistentes y su firma o constancia de la participación). Dichos registros pueden presentarse en formato papel o electrónico. 10) Contar con medidas implementadas para verificar la eficacia de las capacitaciones brindadas.		

Todos los operadores	**4.4.5 Comunicación**	La organización debe: 1) Establecer un procedimiento documentado en el que se establezca la metodología para realizar la comunicación interna y externa sobre la gestión de la seguridad de la cadena de suministro entre los diferentes niveles y funciones de la organización, así como también a sus socios comerciales críticos, autoridades y organismos gubernamentales.	La organización debe establecer un procedimiento para realizar las comunicaciones necesarias a nivel interno (empleados) y externo (socios comerciales, instituciones gubernamentales o no gubernamentales, etc.). Debe realizarse en todos los sentidos y niveles de la estructura organizativa: ascendente, descendente, transversal y horizontal. Asimismo, debe identificar y establecer los flujos, medios, canales, maneras y formas que les permitan transmitir informaciones transparentes, confiables y oportunas de manera comprensible.	• Procedimiento de comunicación.
Todos los operadores Todos los operadores • Exportador • Transportista • Agencia marítima • Agente de carga	**4.5 CONTROL DE LA SEGURIDAD** **4.5.1 Gestión Administrativa** **Documentación de comercio exterior**	La organización debe: 1) Establecer procedimientos documentados o instructivos para la gestión de las operaciones de comercio exterior que realiza, en los que se defina la información necesaria para elaborar los documentos, el procesamiento de la información, los controles realizados para detectar eventuales errores, la forma de conservación y archivo de los documentos, y la manera de acceder a la información en caso de ser requerida. 2) Asegurar el archivo de la documentación de las operaciones de comercio exterior que realice la organización por un período de 5 años, o de acuerdo a la normativa vigente. 3) Asegurar que la información utilizada para despachar y recibir mercaderías (documentos y sistemas informáticos) sea legible, completa, exacta y esté protegida de adulteración o pérdida, y que sea informada a tiempo. Si se utilizan formularios y documentos relacionados con operaciones de importación, exportación y tránsito en formato papel, asegurar que sean protegidos para evitar el uso no autorizado. 4) Asegurar que los manifiestos y los conocimientos de embarque reflejen con precisión la información proporcionada al transportista. Los transportistas deben ejercer la debida diligencia para garantizar que esos documentos sean precisos. 5) Presentar de manera oportuna a la DNA, y de acuerdo a la normativa vigente, los manifiestos y conocimientos de embarque, si corresponde, debiendo reflejar el punto de origen o retiro de la carga por parte del transportista. El peso y la cantidad de bultos deben ser precisos.	El objetivo de contar con procedimientos y controles para la gestión administrativa de comercio exterior, es minimizar eventuales errores que puedan causar que la carga se detenga y así aumentar el riesgo de contaminación. Es importante comprender que el SGS no solo sirve para identificar y minimizar los riesgos, sino que, además, en caso de que ocurra algún ilícito, servirá para deslindar responsabilidades si se cuenta con la trazabilidad completa de las operaciones, y los registros de las actuaciones y controles efectuados por la organización. Se pueden tomar medidas como el uso de archivadores cerrados con llave para restringir el acceso no autorizado a esa documentación. La carga debe describirse con precisión: el peso, las etiquetas, las marcas y el número de bultos o piezas deben ser indicados y verificados. Se espera que el transportista revise la documentación y coteje contra los bultos que están siendo cargados; teniendo en cuenta el tipo de mercaderías a transportar, los materiales de acondicionamiento o embalaje o el tipo de bulto; de manera de saber que estará transportando y si coincide con lo declarado. Algunas de las señales de advertencia de actividades de lavado de dinero y financiamiento del terrorismo podrían ser la voluntad de pagar por encima de la tasa estándar, pago en efectivo, escaso conocimiento de la mercadería que se enviará, evasivas, información de contacto mínima (teléfono	• Procedimientos de las operaciones de comercio exterior que realice la organización. • Seguimiento de operaciones aduaneras, documentación y registros asociados.

		6) Asegurar que el personal revise la información incluida en los documentos de importación/exportación/tránsito para identificar o reconocer envíos de carga sospechosos. 7) Capacitar al personal sobre cómo identificar información en los documentos de envío, en los que podría haber indicios de un envío sospechoso. 8) Para el caso de empresas transportistas, capacitar al personal para revisar los manifiestos y otros documentos a fin de identificar o reconocer envíos de carga sospechosos, tales como: - aquellos que se originan o tienen destinos inusuales, - aquellos pagados en efectivo o cheques, - utilización de rutas no habituales que evidencien prácticas inusuales de envío o recepción, - información vaga, generalizada o faltante. 9) Tener en cuenta, en función de su análisis de riesgo, indicadores clave de advertencia para actividades de lavado de dinero y financiamiento del terrorismo más aplicables de acuerdo a la modalidad de negocio y su rol en la cadena de suministro.	celular, destinatario), empresa nueva o sin antecedentes comerciales, etc. Las técnicas más utilizadas para el lavado de activos en el comercio exterior son: a) sobrefacturación y subfacturación de bienes y servicios. b) facturación múltiple de bienes y servicios. c) alteración del volumen de embarques. d) adulteración de la descripción de los bienes y servicios.	• Capacitaciones brindadas al personal.
Todos los operadores				•Matriz de riesgo. • Registro de evaluación de las cadenas de suministro y evaluación de riesgos internacionales.

Todos los operadores	**4.5.2 Seguridad en relación a los socios comerciales**	La organización debe: 1) Establecer procedimientos documentados basados en riesgos para: a) la selección de socios comerciales confiables (clientes y proveedores), b) el monitoreo de clientes y proveedores, tanto actuales como nuevos que incorpore la organización, y c) la evaluación de los proveedores. 2) Definir criterios para la selección de clientes y proveedores, la información que se investigará y se le solicitará a los socios, la forma en la que se verificará esa información, y los criterios para aceptar o rechazar la relación comercial. 3) Llevar a cabo verificaciones de los antecedentes de los socios comerciales críticos, incluyendo verificaciones vinculadas a involucramiento en actividades ilícitas y controles en lavado de activos y financiamiento del terrorismo. Dicha verificación debe incluir comprobaciones en las fuentes de información o listados emitidos por organismos gubernamentales nacionales o extranjeros, u organismos internacionales. En el caso de que una organización o persona que figure en esos listados parezca coincidir con una parte potencialmente involucrada en una operación de comercio exterior, se debe llevar a cabo una investigación adicional antes de continuar. Se debe considerar informar a la autoridad pertinente, sobre estas organizaciones o personas incluidas en estas listas y/o de las operaciones que las mismas pretenden realizar. 4) Incluir verificaciones de sus socios comerciales para evitar que sus bienes importados o comercializados sean extraídos, se produzcan o fabriquen, total o parcialmente, con formas de trabajo prohibidas, tales como trabajo forzado, bajo condiciones de reclusión o trabajo infantil. 5) Verificar el emplazamiento de los socios comerciales a través de visitas a las instalaciones, u otras medidas equivalentes que correspondan. 6) Tomar en consideración en el proceso de selección de socios comerciales, si el socio es miembro de un Programa de Operador Económico Autorizado – OEA, o con el que la DNA haya firmado un Acuerdo de Reconocimiento Mutuo. La certificación OEA se considera una prueba aceptable para cumplir con los requisitos de socios comerciales del Programa OEC para establecer un vínculo confiable y seguro. 7) Obtener evidencia de la certificación de sus socios comerciales (copia del certificado OEA) y continuar monitoreando su situación para asegurarse que mantengan su certificación. 8) Solicitar a los socios comerciales proveedores que no cuenten con una certificación en un Programa OEA, un compromiso formal de que cumplen con los requisitos de seguridad que le sean aplicables, realizar auditorías, cuestionarios, u otras medidas equivalentes para verificar su cumplimiento y actualizar el análisis de riesgo de la organización. 9) Solicitar a los proveedores extranjeros que cumplan con el requisito de seguridad de las unidades de transporte de carga y de seguridad de las mercaderías desde el punto de origen.	La seguridad en relación a los socios comerciales refiere a aquellos riesgos asociados a clientes y proveedores. El análisis de riesgo resulta la herramienta adecuada para determinar cuáles son aquellos clientes y proveedores críticos que merecen atención especial. Para mitigar los riesgos se debe establecer un procedimiento escrito en el que se describa el proceso de selección de socios comerciales (conviene tener un procedimiento para clientes y otro para proveedores), estableciendo una metodología de análisis de riesgo para la selección, definiendo la información que se le solicitará a los socios para su análisis, y de esta manera determinar la criticidad de los mismos. Se debe hacer un seguimiento basado en riesgo del socio y una actualización periódica, tanto de los socios comerciales con los cuales la organización ya se vinculaba, como con los nuevos. En general las organizaciones están acostumbradas a definir especificaciones y solicitar información a los proveedores, pero no resulta una práctica habitual definir criterios para aceptar clientes. Los siguientes son ejemplos de algunos de los elementos de investigación que pueden ayudar a determinar si una empresa está legalmente constituida: • Verificar la dirección comercial de la empresa y cuánto tiempo ha estado en esa dirección; • Realizar investigaciones en Internet sobre la empresa y sus autoridades (por ejemplo, consultar páginas web: https://e-justice.europa.eu/content_find_a_company-489-en.do?clang=en, https://www.societe.com/, https://www.score3.fr, Creditsafe.com, Orbis.com); • Verificación de referencias comerciales; • Verificar el emplazamiento (visitas, verificación en Google Earth); • Búsqueda de noticias. Se incorpora un nuevo enfoque en la verificación y selección de los socios comerciales que refiere a las verificaciones sobre trabajo forzado/trabajo infantil y lavado de activos y financiamiento del terrorismo (LAFT). Para la verificación relacionada a las medidas contra el trabajo forzado / infantil o bajo condiciones de encarcelamiento, puede tomarse como insumo el cuestionario de socios comerciales, en el que se incorporen preguntas relacionadas al cumplimiento del mismo, o certificaciones internacionales en la materia. A efectos de verificar la información relacionada a LAFT de los socios comerciales, en el sitio web de la Secretaría Nacional para la Lucha contra el Lavado de Activos y Financiamiento del Terrorismo (SENACLAFT) se encuentran	• Procedimiento de socios comerciales (clientes y proveedores). •Matriz de riesgo. • Registro de evaluación de las cadenas de suministro y evaluación de riesgos internacionales. • Registro/legajo de cada cliente/proveedor que incluya, entre otros: • Datos de contacto. • Evidencia de la información verificada: 1- Emplazamiento (Registro de visita u otro medio utilizado). 2- Búsquedas en Internet. 3- Referencias comerciales. 4- Verificación listados LAFT 5- Copia de certificaciones OEA. • Compromiso de seguridad. • Cuestionario de socios comerciales. • Informes de auditoría. • Envío de la política de seguridad. • Compromiso de confidencialidad. • Contrato de servicios. • Capacitaciones a proveedores.

		10) Asegurar el cumplimiento de los criterios de seguridad por parte de sus proveedores, especialmente en los casos de subcontratación de sus procesos en las cadenas de suministros, cumpliendo con los requisitos OEC que le apliquen de acuerdo al servicio brindado, mediante auditorías, visitas, cuestionarios, u otras medidas equivalentes. 11) Actualizar las evaluaciones de seguridad de sus socios comerciales de forma regular, de acuerdo a las circunstancias, ocurrencia de incidentes de seguridad, o identificación de nuevos riesgos, para garantizar que continúan cumpliendo con los criterios de seguridad. 12) Abordar lo antes posible las vulnerabilidades que se identifiquen durante las evaluaciones de seguridad de los socios comerciales, e implementar las correcciones que correspondan, de manera oportuna. Se debe comprobar que las vulnerabilidades se han mitigado mediante pruebas documentales.	listados una serie de fuentes de información abiertas para consulta pública: https://www.gub.uy/secretaria-nacional-lucha-contra-lavado-activos-financiamiento-terrorismo/comunicacion/publicaciones/fuentes-informacion En el procedimiento se debe hacer referencia a la certificación en Programas OEC/OEA como un elemento de análisis para la selección de socios comerciales. Para verificar la vigencia de la certificación se deberá contar con el registro correspondiente, solicitando a los socios comerciales el certificado que lo acredite, y consultando el sitio web de la DNA o de la administración aduanera extranjera donde se listan los nombres de las empresas OEA certificadas por la misma. https://www.aduanas.gub.uy/innovaportal/v/22569/14/innova.front/acuerdos-de-reconocimiento-mutuo-arm.html Aquellos proveedores definidos como críticos para la seguridad de la cadena de suministro deben ser informados sobre el Programa OEC y los requisitos de seguridad que la organización cumple. La organización debe definir los requisitos de seguridad que le apliquen a sus proveedores, dependiendo del tipo de operador o servicio que brinde, suministrar formalmente dicha información mediante una declaración por escrito la cual deberá estar firmada por un responsable de la organización, y ser devuelta firmada por el proveedor en señal de aceptación de la misma. En dicho documento se deberá solicitar al proveedor aceptar suministrar información, recibir visitas y auditorías, e implementar las medidas de seguridad que le correspondan. Para el caso de aquellos proveedores que manejan directamente la carga y/o la documentación de importación/exportación/tránsito internacional, es fundamental que la organización se asegure que dichos socios comerciales cuenten con las medidas de seguridad adecuadas para proteger los bienes a lo largo de la cadena de suministro internacional. Asimismo, se podrá establecer el cumplimiento de dichos requisitos en el contrato de servicio. Las empresas importadoras deben asegurar que los proveedores del exterior realicen la verificación de las unidades de transporte de carga y de la mercadería, tal como se explicita en el requisito 4.5.3 y 4.5.5, debiendo solicitar la evidencia de lo realizado. La organización debe tener un procedimiento documentado en el que se describa la metodología de evaluación de sus socios comerciales proveedores. Dicha evaluación debe comprender el análisis del grado de cumplimiento de los	• Otros que la organización implemente.

			requisitos de seguridad que le apliquen. Las organizaciones deben asegurarse que sus proveedores desarrollen los procedimientos de seguridad de acuerdo con los requisitos que le sean aplicables. Para ello se debe obtener información mediante el envío de un cuestionario de seguridad para que sea completado por el proveedor, realizar visitas y auditorías. En el caso del cuestionario, el mismo debería pedir a los proveedores que describan las medidas de seguridad para cada uno de los requisitos de seguridad que le apliquen, siendo de suma importancia solicitar la evidencia del mismo. De esta manera se deberá realizar una evaluación documentada de los riesgos para verificar que los proveedores que no sean OEC/OEA cumplan con los requisitos de seguridad. Los riesgos identificados serán las debilidades encontradas en el cumplimiento de los requisitos. Cada operador podrá establecer un sistema de clasificación del riesgo de la seguridad más conveniente en base a su modelo de negocio. Si se encuentran debilidades se deberá definir un plan de acción para la implementación de las medidas de seguridad. Se debe contemplar el tiempo y los recursos que requiera dicha implementación. Por ejemplo, la instalación de un sistema de cámaras de vigilancia suele llevar más tiempo que un cambio de procedimiento, pero la debilidad en seguridad debe abordarse en el momento del hallazgo. En este sentido, si el problema es reemplazar una cerca dañada, el proceso para comprar una nueva cerca o reparar la ya existente debe comenzar de inmediato (abordar la debilidad) y la instalación de la nueva cerca (la acción correctiva) debe realizarse tan pronto como sea factible. Según el nivel de riesgo involucrado y la importancia de la debilidad encontrada, algunos problemas pueden requerir atención inmediata. Si se trata de una deficiencia que puede poner en peligro la seguridad de un contenedor, por ejemplo, debe abordarse lo antes posible. Para asegurar que las debilidades fueron subsanadas, se debe solicitar al proveedor las evidencias que den cuenta de ello. Algunos ejemplos de evidencia documental pueden incluir registros de verificación de las instalaciones, registros fotográficos o fílmicos, registro de incidentes o acciones correctivas, solicitudes de reparación, etc. Las empresas tienden a tercerizar una gran parte de las actividades de su cadena de suministro y, en este caso, deberán exigir a sus proveedores que implementen las medidas de seguridad. Para aquellos proveedores que no tengan una certificación en un Programa OEC/OEA, y a su vez subcontraten un servicio para manipular la mercadería de un operador (por ej. un transportista que subcontrata a otro o el operador contrata a	

			una empresa para que proporcione personal- pandilla) se deberá garantizar que estos proveedores tercerizados cumplan con los criterios de seguridad que le sean aplicables. Para verificar el cumplimiento de los requisitos, la organización deberá estar en conocimiento de esta modalidad de subcontratación de su proveedor, y deberá incluirlo en el análisis de riesgo. Los proveedores y las empresas subcontratadas por éstos, deben recibir formación en materia de seguridad en función del servicio que presten. La organización debe actualizar el análisis de riesgo de sus socios comerciales una vez al año, cuando se identifique un nuevo riesgo o cuando se produzca un incidente de seguridad.	
• Exportador • Importador • Depósito • Zona franca • Usuario de ZF • Transportista • Terminal de carga • Operador portuario (*)Agencia marítima (en caso de manipular la mercadería) (*) Agente de carga (en caso de manipular la mercadería) (**) Despachante de aduana (en caso de contratar servicios de transporte debe trasladar el requisito al proveedor)	**4.5.3** **Seguridad en las unidades de transporte de carga e instrumentos de tráfico internacional (ITI)**	La organización debe: 1) Establecer procedimientos documentados para la inspección de las unidades de transporte de carga e ITI, con criterios definidos de aceptación y rechazo, estableciendo los puntos vulnerables a inspeccionar. 2) Implementar un proceso de inspección que incluya procedimientos documentados para las inspecciones de seguridad y agrícolas. 3) Realizar inspecciones de seguridad y agrícolas a todas las unidades de transporte e ITI al recibir las cargas de importación, para garantizar que sus estructuras no hayan sido modificadas para ocultar contrabando, o que hayan sido contaminadas con plagas agrícolas visibles. 4) Realizar inspecciones de seguridad y agrícolas a todas las unidades de transporte e ITI antes de la carga/llenado/embalado, para garantizar que sus estructuras no hayan sido modificadas para ocultar contrabando, o que hayan sido contaminadas con plagas agrícolas visibles. 5) Realizar dichas inspecciones de las unidades de transporte e ITI de manera sistemática, en playas de estacionamiento de unidades de transporte y/o áreas restringidas, delimitadas y de acceso controlado, debiendo ser monitoreadas a través de un sistema de circuito cerrado de televisión (CCTV). Estas inspecciones deben ser realizadas también luego de permanecer en espera, y/o en caso de paradas intermedias hacia su destino. 6) Lavar/aspirar las unidades de transporte e ITI en caso de encontrar contaminación visible de plagas durante la inspección, para eliminar la misma. 7) Mantener las unidades de transporte e ITI en un área segura durante la carga, espera o almacenamiento para evitar el acceso no autorizado que pudiera resultar en una alteración de la estructura de un ITI, o que el precinto o las puertas se vean comprometidos.	La seguridad en las unidades de transporte (UT) de carga pretende evitar que medios de transporte e ITI sean manipulados para ocultar mercadería ilícita o poder abrirlos sin dejar rastros. La prevalencia de los planes de contrabando que implican la modificación de las UT o ITI hace que sea imperativo que los conductores realicen inspecciones de los mismos para buscar deficiencias estructurales graves. Debe establecerse en los procedimientos: a) la forma de inspección (puntos vulnerables), b) los criterios de aceptación y rechazo de las unidades de transporte de carga c) contar con un registro para cada una de las unidades de transporte de carga que la organización utiliza en sus operaciones (atendiendo a los diferentes tipos de unidades/ contenedores, sus diferentes vulnerabilidades, medidas estándar, etc.). d) capacitación: los conductores y el resto del personal que realiza las inspecciones de seguridad de los medios de transporte vacíos y de los ITI deben estar capacitados para inspeccionarlos con el debido enfoque en seguridad. Se requiere además que el procedimiento incluya una guía de cómo se inspeccionan las UT e ITI, incluyendo aspectos agrícolas (lo más visible: plagas, insectos, material orgánico). Para realizar la inspección agrícola no se requiere de equipo especializado. La organización debe asegurar que las unidades de carga estén limpias antes del proceso de carga, y que estas sean inspeccionadas para evitar la contaminación	•Procedimiento de seguridad en las UT e ITI. •Registro de inspección de UT y/o ITI. •Registros fílmicos de la inspección y/o fotográficos. •CCTV. •Registro de reparación de lonas.

		8) Incluir en las inspecciones sistemáticas: Tractor y remolque: 1. Parachoques. 2. Motor. 3. Neumáticos/llantas. 4. Piso. 5. Tanque de combustible. 6. Cabina. 7. Tanques de aire. 8. Eje trasmisión. 9. Quinta rueda. 10. Chasis/exterior. 11. Piso interior. 12. Puertas internas/externas. 13. Paredes laterales. 14. Techo exterior/interior. 15. Pared frontal. 16. Unidad de refrigeración. 17. Tubo de escape. 9) Establecer y mantener registro e historial de reparación de las lonas para las unidades de transporte en las que se utilice la modalidad de enlonado. 10) Inspección de ITI: Contenedores y dispositivos de carga unitaria (DCU) Realizar una inspección de siete puntos en todos los contenedores vacíos y DCU, y una inspección de ocho puntos en todos los contenedores refrigerados vacíos y DCU antes de la carga/llenado incluyendo: 1. Pared frontal. 2. Lado izquierdo. 3. Lado derecho. 4. Piso interior y exterior. 5. Techo interior y exterior. 6. Puertas interiores/exteriores, incluida la fiabilidad de los mecanismos de cierre de las puertas. 7. Exterior/chasis/travesaños. 8. Caja del ventilador en contenedores refrigerados. 11) Inspeccionar completamente las unidades de transporte e ITI (según corresponda). El mecanismo de cierre debe resistir razonablemente los intentos de quitarlo: las puertas, las manijas, las varillas, los cerrojos, los remaches, los soportes y todas las demás partes del mecanismo de bloqueo de un contenedor deben inspeccionarse completamente para detectar manipulaciones y cualquier inconsistencia en el mismo antes de colocar cualquier dispositivo de precintado. 12) Registrar la inspección de todas las unidades de transporte e ITI vacíos en una lista de verificación que incluya los siguientes elementos: • Número de contenedor/ITI. • Matrícula de tractor y remolque. • Empresa transportista. • Hora de ingreso del camión y nombre del conductor.	visible por plagas, restos de desechos, residuos y otros materiales, incluyendo elementos naturales. Las áreas donde permanezcan camiones de exportación cargados deben de tener las medidas de seguridad que se señalan en el requisito 4.5.7 “Seguridad física en las instalaciones” y 4.5.8 “Seguridad en el acceso de personas”. Para el caso de los camiones, la inspección debe prever variedad de lugares donde eventualmente se puede ocultar carga ilícita. Incluso pudiendo realizar una inspección exhaustiva del camión al momento de la carga, siempre existe el riesgo de que la mercadería ilícita se introduzca durante el trayecto a frontera. En este sentido, es mucho más importante los controles y registros que se realicen previamente sobre la empresa transportista, y cómo ésta selecciona, capacita y monitorea a su personal, además de tener los registros del trayecto realizado por el camión, paradas realizadas, tiempos de tránsito, etc. Se recomienda como mejor práctica la utilización de la metodología de los 17 puntos de inspección del tractor y remolque. Para el caso de las empresas transportistas, deben mantener un registro del mantenimiento realizado a las lonas, de manera de poder diferenciar una reparación realizada por la empresa, de un corte enmendado que se haya realizado durante el trayecto. La inspección previa a la carga es fundamental para comprobar la integridad de la unidad de carga y mitigar el riesgo de transporte simultáneo no autorizado de otros productos. Permite la detección, por ejemplo, de paredes falsas en contenedores o carrocerías. La evaluación del operador deberá cubrir, en su caso, los procedimientos realizados por un tercero. Los contenedores deben someterse a inspecciones de siete puntos; en los contenedores refrigerados se debe revisar un octavo punto, que es la carcasa del ventilador. Es preciso registrar todos los controles que se hagan sobre las medidas del contenedor, puertas, bisagras, sistemas de cierre, reparaciones realizadas, etc. Detectar espacios ocultos requiere de conocimiento y experiencia y saber interpretar indicios como olor a pintura o a metal quemado por una reciente soldadura. Las inspecciones de supervisión de los medios de transporte se realizan para contrarrestar las conspiraciones internas y verificar que las inspecciones se realicen de acuerdo a lo establecido. Como práctica recomendada, los supervisores pueden ocultar un artículo (como un bulto o una caja) en el medio de transporte para determinar si el funcionario que realiza la inspección lo encuentra. Esto podría ser realizado por un	

		• Fecha y hora de la inspección. • Los puntos de las unidades de transporte e ITI que fueron inspeccionados. • Número de precinto, verificación realizada del procedimiento VVTT. • Inspección agrícola. • Nombre y firma del empleado que realiza la inspección. Si las inspecciones son supervisadas, el supervisor también debe firmar la lista de verificación. 13) Realizar y documentar verificaciones aleatorias de las unidades de transporte por parte de los supervisores o encargados del área, en función del riesgo, después de que el personal designado haya realizado las inspecciones. Dichas verificaciones deben realizarse periódicamente, y con mayor frecuencia en función del riesgo. 14) Realizar verificaciones al azar y sin previo aviso para que no se vuelvan predecibles, en varios lugares donde la unidad de transporte es susceptible de contaminación: patios de carga, después de que haya sido cargada la mercadería, y en caso de paradas intermedias hacia su destino, a efectos de detectar contaminación de la carga, producto de conspiraciones internas. 15) Incorporar en el paquete de documentación de envío el registro de inspección completo de contenedores/ITI. El consignatario debe recibir el paquete de documentación de envío completo, antes de recibir la mercadería. 16) Las empresas de transporte terrestre deben contar con un sistema de seguimiento satelital (GPS o similares), y guardar los correspondientes registros de las operaciones. 17) Requerir a los proveedores de transporte el acceso a los sistemas de seguimiento satelital para el rastreo de los medios de transporte desde el origen hasta el punto de destino final. 18) Incorporar en los acuerdos de servicio con dichos proveedores los requisitos específicos para el seguimiento, la notificación y el intercambio de datos. 19) Contar con sistemas y procedimientos documentados para responder a desviaciones significativas de rutas y llegadas tardías a las áreas de carga, puntos de transferencia o destino final, para el caso de transportistas. Para la carga terrestre de exportación se deben indicar las paradas autorizadas, evitando paradas innecesarias. 20) Notificar al remitente/exportador sobre cualquier retraso significativo en la ruta debido al clima, el tráfico y/o cambio de ruta. El remitente/exportador debe verificar independientemente la causa del retraso. 21) Alertar (tan pronto como sea posible) a cualquier socio comercial en la cadena de suministro que pueda verse afectado y a las autoridades competentes, según corresponda, si se descubre una amenaza potencial (o detectada) a la seguridad de un envío o medio de transporte.	encargado de seguridad, a quien se le hace responsable ante la alta gerencia por la seguridad, u otro miembro del personal de administración designado. El seguimiento de los medios de transporte se realiza para evitar su desvío y alteración de la carga o de la estructura del medio de transporte o ITI, evitando la introducción de mercadería ilícita. Conforme al riesgo, corresponde que los proveedores de transporte realicen el seguimiento de sus medios de transporte o ITI en tiempo real y compartan la información con el exportador/remitente. La carga en reposo es carga en riesgo. Las paradas programadas también deben considerarse en un procedimiento general de seguimiento y vigilancia, así como la notificación de retrasos en las rutas.	

• Exportador • Depósito • Usuario de ZF • Transportista • Terminal de carga • Operador portuario • Agencia marítima (*) Agente de carga (en caso de manipular la mercadería)	**4.5.4** **Seguridad de los precintos**	La organización debe: 1) Establecer procedimientos documentados para la utilización de precintos de alta seguridad, que describan cómo se gestionan y controlan los precintos en las instalaciones y durante el transporte. 2) Establecer en los procedimientos los pasos a seguir para reconocer y denunciar la adulteración o uso fraudulento de los precintos, es decir, si se descubre que un precinto está adulterado, manipulado o tiene el número incorrecto, investigar las causas del incidente, incluyendo la documentación correspondiente y los protocolos de comunicación a los socios comerciales. 3) Documentar los hallazgos de la investigación, definir e implementar las medidas correctivas que correspondan, registrar lo realizado, incluyendo las consecuentes modificaciones de los procedimientos involucrados y verificar su eficacia. Cualquier acción correctiva debe implementarse lo más rápido posible. 4) Mantener estos procedimientos fácilmente accesibles para las áreas operativas 5) Revisar los procedimientos al menos una vez al año y actualizarlos según sea necesario. 6) Incluir los siguientes elementos en la gestión y control de precintos: a) Control de acceso a los precintos: • Gestión de los precintos restringida al personal autorizado. • Almacenamiento seguro, mantener en un área de acceso restringido. b) Inventario de precintos, distribución y seguimiento (registro de precintos): • Registro de la recepción de nuevos precintos. • Registro de entrega de precintos. • Seguimiento y control de los precintos. • Colocación de los precintos solo por personal capacitado y autorizado. • Utilización de forma aleatoria. c) Control de los precintos para el transporte: • Al retirar el ITI precintado (o después de detenerse), se debe verificar que el precinto esté intacto y sin signos de manipulación. • Se debe confirmar que el número del precinto coincida con lo que se indica en los documentos de envío. d) Precintos rotos durante el transporte: • Si se examina la carga por parte de una autoridad competente y se rompe el precinto original, se debe registrar el número de precinto de reemplazo. El conductor debe notificar de inmediato al área de seguimiento de operaciones de su empresa cuando se rompa un precinto, indicar quién lo rompió y proporcionar el nuevo número de precinto. • La empresa transportista debe notificar inmediatamente al remitente/exportador/importador/despachante de aduana sobre el cambio de precinto y el número de precinto de reemplazo. • El remitente/exportador debe tomar nota del número del precinto de reemplazo en el registro de precintos, cuando corresponda.	El control de los precintos pretende evitar que éstos puedan ser “clonados” y utilizados para no dejar evidencia de que la carga fue violada. Los precintos deben guardarse bajo llave, debe registrase su uso, mantener un control de inventario, y deben usarse con un orden arbitrario, no en orden numérico. Cuando los precintos se reciben de parte de la agencia naviera o de un tercero, deberían recibirse en un sobre lacrado y mantenerse en un área restringida hasta su uso. Los controles de los precintos deben estar documentados, y todo el personal afectado debe ser formado y supervisado para garantizar el cumplimiento de las políticas y procedimientos de seguridad de los precintos. Se deben tomar pruebas documentadas del precinto correctamente instalado (por ejemplo, fotografías digitales) en el punto de carga. Estas imágenes deben enviarse electrónicamente al lugar de destino con fines de verificación. La seguridad de los precintos incluye tener un procedimiento de precintos completo, documentado, que aborde todos los aspectos de su seguridad, incluyendo los precintos que cumplan la norma ISO 17712. Para el caso de camiones enlonados, la colocación de precintos debe aplicarse a un cable continuo que recorra el perímetro del camión y que permita dejar evidencia en caso de ser violado.	•Procedimiento seguridad de los precintos. •Registro inventario de precintos. •Registro de inspección de UT y/o ITI. •Registro fotográfico de cierre de la UT o ITI con precinto, en auditoria testigo de operaciones aduaneras. • Registro de auditorías para el control de los precintos. •Certificaciones de precintos ISO 17712.

		En caso de hallar discrepancias se debe: • Retener cualquier precinto que se detecte que haya sido adulterado o falsificado, para ayudar en la investigación. • Investigar la discrepancia y hacer un seguimiento con medidas correctivas (si se justifica). • Según corresponda, reportar los precintos comprometidos a la DNA y ésta a la aduana de destino para ayudar en la investigación. 7) Asegurar todas las cargas que se puedan precintar, inmediatamente después de la carga/relleno por parte del responsable (remitente) con un precinto de alta seguridad que cumpla o exceda las normas más recientes de la Organización Internacional de Normalización (ISO) Norma 17712 para precintos de alta seguridad. Son aceptados los precintos de pernos y cables que cumplan la norma mencionada. 8) Documentar que los precintos de alta seguridad que se utilicen cumplan o excedan el estándar ISO 17712 más actual. 9) Colocar todos los precintos de forma segura y de manera adecuada a los ITI que transportan carga. 10) Realizar por parte de la gerencia o un supervisor de seguridad, auditorías al inventario de precintos, incluyendo una revisión periódica de los precintos almacenados y la conciliación de los registros de inventario de precintos con los documentos de envío. Dichas auditorías deben estar documentadas. 11) Verificar periódicamente los números de precintos colocados en los medios de transporte e ITI, como parte de las auditorias de precintos que deben realizar los gerentes o supervisores. 12) Seguir el proceso VVTT de verificación de precintos para garantizar que todos los precintos de alta seguridad se hayan colocado correctamente en los ITI: V - Ver mecanismos de cierre de precintos y contenedores, asegurarse de que estén bien; V - Verificar el número de precinto con los documentos de envío para cotejar su precisión; T: Tirar del precinto para asegurarse que esté colocado correctamente; T: Torcer: girar y dar vuelta el precinto del perno para asegurarse que sus componentes no se desenrosquen, se separen entre sí o que alguna parte del precinto se afloje. 13) Establecer una metodología para la destrucción de los precintos utilizados, rotos o descartados. 14) En caso de utilizar otro sistema de precintos que sea aprobado por la DNA, documentar de qué manera garantizan y aseguran la integridad de la carga, de las unidades de transporte e ITI.		

• Exportador • Importador • Depósito • Zona franca • Usuario de ZF • Terminal de carga • Operador portuario (*) Agente de carga (en caso de manipular la mercadería)	**4.5.5 Seguridad de las mercaderías**	La organización debe: 1. Establecer procedimientos documentados para controlar y registrar las sucesivas etapas del movimiento de mercaderías (empaque, almacenamiento, carga, transporte, tiempos de tránsito, etc.). 2. Controlar y registrar el uso de los materiales de empaque para evitar un uso indebido de los mismos (cajas, etiquetas, cintas con logo, etc.). 3. Registrar los procesos de carga incluyendo personal interviniente, responsable, datos del medio de transporte y del conductor, fotos y/o videos del estado de la carga, así como también del proceso de cierre y precintado del medio de transporte y/o ITI. Dichas imágenes deben enviarse electrónicamente al destino para fines de verificación. Los importadores deberán trabajar con sus proveedores en el exterior a efectos de asegurarse la obtención de dicha información y registros. 4. Restringir el acceso a las áreas de empaque y carga de mercadería al personal autorizado, y contar con una supervisión permanente durante estos procesos. 5. Controlar el proceso de carga en contenedores o ITI por un supervisor de área u otro funcionario designado a esos efectos. 6. Tomar medidas para proteger la carga de accesos no autorizados cuando la misma se almacena durante la noche o durante un período de tiempo prolongado. 7. Inspeccionar con regularidad las áreas de almacenamiento de carga y las áreas circundantes inmediatas para garantizar que las mismas permanezcan libres de contaminación visible por plagas. 8. Efectuar la entrega de la mercadería al consignatario o a otras personas que acepten la misma, en un área específica que deberá estar monitoreada. 9. Investigar y resolver todas las discrepancias, faltantes o sobrantes, o anomalías significativas, según corresponda. 10. Conciliar la carga que arriba con la información del manifiesto de carga. 11. Verificar la carga de salida con las órdenes de compra o entrega. 12. Comunicar al destinatario antes de la salida, los números de precintos asignados a los envíos. 13. Incluir los números de precintos, plasmándose electrónicamente en el conocimiento de embarque u otros documentos de envío.	La seguridad de las mercaderías, al igual que lo señalado para las unidades de transporte de carga, tiene por objeto evitar que estas puedan ser manipuladas para ocultar mercadería ilícita. Los procedimientos definidos y los registros utilizados, deben asegurar el control y trazabilidad de la mercadería a lo largo de toda la cadena logística, de manera de evitar que la carga sea contaminada y, en caso de que esto ocurra, contar con la información de quiénes, cuándo y dónde tuvieron contacto con la mercadería. Para definir el alcance de los controles, es preciso comprender que los riesgos de contaminación comienzan cuando se conoce el destino específico de una mercadería. A partir de ese momento, la carga puede ser contaminada durante la preparación o acondicionamiento para la exportación, el proceso de carga y/o durante el transporte. Los puntos críticos son cuando la carga permanece detenida y sin supervisión directa. Un aspecto vulnerable que debe ser periódicamente controlado por las empresas es el empaque. Un práctica común para contaminar la carga es intercambiando una caja previamente preparada con mercadería ilícita por otra con la mercadería de exportación. Por esta razón se deben tener bajo control las cajas, cintas de empaque, etiquetas y precintos. El acceso restringido a las áreas de carga, la identificación del personal involucrado, las fotografías y videos para registrar el proceso de carga son importantes en el control de la mercadería. Cuando sea posible, cambiar arbitrariamente algún tipo de identificación en cada exportación, como ser el color de la etiqueta o de la cinta de empaque, reduce el riesgo de que cajas previamente preparadas, puedan ser intercambiadas fácilmente. A efectos de asegurar un área de almacenamiento o de estacionamiento de unidades libre de plagas, se pueden usar medidas preventivas como cebos, trampas u otras barreras, eliminación de malezas, o vegetación abundante.	•Procedimientos que incluyan las distintas etapas del movimiento de mercaderías, gestión de materiales de empaque y cintas con logo, almacenamiento y entrega. •Registro fílmico fotográfico del proceso de carga, cierre y precintado de la UT o ITI. •Registro de control y uso de materiales de empaque. •Control de acceso a áreas restringidas. •Registro de discrepancias faltantes o sobrantes. •Registros que se establezcan para el control de la documentación y verificación de la carga. •Otros que la organización implemente. •Constatación en recorrida por instalaciones.

• Exportador • Importador • Depósito • Zona franca • Usuario de ZF • Transportista • Terminal de carga • Operador portuario (*)Agentes de carga (en caso de manipular la mercadería)	**4.5.6** **Seguridad agrícola**	La organización debe: 1. Establecer procedimientos documentados para prevenir la contaminación por plagas incluyendo el cumplimiento de la normativa sobre Materiales de Embalaje de Madera. 2. Cumplir con las Normas Internacionales para Medidas Fitosanitarias (NIMF 15) de la Convención Internacional de Protección Fitosanitaria (CIPF) y la normativa nacional vigente en la materia. 3. Cumplir las medidas de prevención de plagas visibles en toda la cadena de suministro.	En términos de manejo de plagas, la inclusión de este requisito dentro del Programa OEA se enfatiza en la prevención a través de procedimientos de sanidad, especialmente porque la introducción de una plaga o contaminante mayor causa un daño muy importante a la economía del país, siendo ocasionada generalmente por accidente y no por un acto deliberado. La DNA también tiene el rol de vigilar el cumplimiento de esta normativa, en particular según lo establecido en el Decreto 156/006 mediante el cual se internaliza la NIMF No.15. La normativa fitosanitaria internacional presta particular atención a ciertas maderas, que si bien no constituyen mercaderías en sí mismas, acompañan el traslado de otras mercaderías transportadas, protegidas o sujetadas, que requieren de los denominados materiales de embalaje, soporte y estiba. Los mismos incluyen cajas, cajones, bobinas, contenedores, jaulas, listones y pallets que en su mayor parte son confeccionados en madera por adaptarse a los principios de la ingeniería del diseño, su variedad de condiciones de uso y su bajo costo. Por tal razón, están sujetos a una serie de requisitos fitosanitarios que trascienden el tipo de producto comercializado con el que se relacionan. La NIMF No.15 “Directrices para reglamentar el embalaje de madera utilizado en el comercio internacional”, describe los procedimientos fitosanitarios para reducir el riesgo de introducción y/o dispersión de plagas cuarentenarias asociadas a estos materiales, que comprenden medidas a largo y corto plazo y medidas adicionales. La organización debe asegurarse de utilizar materiales de embalaje que cumplan con lo establecido en la normativa vigente sobre el tratamiento de embalajes de madera y su correspondiente certificación.	•Procedimiento que incluya el uso y control de material de embalaje apto acorde a la normativa vigente. •Verificación de la marca de certificación de embalaje de madera. •Registros de inspección de UT e ITI

Todos los operadores	**4.5.7 Seguridad físicas en las instalaciones**	La organización debe: 1. Establecer procedimientos documentados que describan las medidas de seguridad para garantizar la integridad de las instalaciones, e impedir el acceso no autorizado a las mismas. 2. Definir e identificar las áreas críticas o sensibles para establecer su acceso restringido. 3. Contar en sus instalaciones con un cerco perimetral que impida los accesos no autorizados. 4. Contar con barreras físicas y/o elementos disuasorios que impidan el acceso no autorizado a las instalaciones de manipuleo, almacenamiento y las playas de estacionamiento. 5. Contar con barreras interiores para asegurar la carga y las áreas de manipulación. De acuerdo al análisis de riesgo, las barreras interiores adicionales deben separar los diferentes tipos de cargas (nacionales, internacionales, de alto valor, peligrosas). 6. Vigilar las puertas por donde ingresan y egresan vehículos y/o personal (así como otros puntos de salida). El personal y los vehículos podrán estar sujetos a revisión al ingreso y a la salida de las instalaciones. 7. Separar y controlar el acceso desde los vestuarios del personal a las áreas de almacenaje, acondicionamiento y carga. 8. Identificar y separar las áreas de estacionamiento de vehículos privados de las de manipulación, almacenaje y carga de mercaderías. 9. Prohibir que los vehículos privados se estacionen en o junto a las áreas de manejo y almacenamiento de carga y medios de transporte. 10. Verificar que todas las ventanas y puertas de las áreas críticas cuenten con cerraduras; registrar y controlar las llaves y códigos o tarjetas de acceso entregadas. 11. Contar con una iluminación externa e interna que permita realizar una vigilancia adecuada de entradas, salidas, áreas de manipulación y almacenamiento, cercos y áreas de estacionamiento. 12. Contar con sistemas de tecnología de seguridad para monitorear las instalaciones y evitar el acceso no autorizado a áreas sensibles (sistemas de alarma y videocámaras necesarios, acorde a la extensión y complejidad de las áreas a vigilar). 13. Contar con procedimientos documentados que establezcan el uso, mantenimiento y protección de esta tecnología. 14. Incluir en los procedimientos los siguientes aspectos: • Limitar el acceso a los lugares donde se controla/administra la tecnología, o donde se guarda su hardware (centro de monitoreo, paneles de control, unidades de grabación de video, etc.) únicamente al personal autorizado. • Implementar medidas para probar/inspeccionar la tecnología de manera regular. • Incluir inspecciones para verificar el correcto funcionamiento del equipo y, si corresponde, que el equipo está colocado correctamente. • Documentar los resultados de las inspecciones y las pruebas de testeo. • En caso de ser necesarias acciones correctivas, implementarlas y documentarlas oportunamente.	La organización debe contar con procedimientos escritos que garanticen la seguridad en sus instalaciones, implementando medidas de seguridad en todas las zonas de alto riesgo, para garantizar que las estructuras estén adecuadamente protegidas contra el acceso o las actividades no autorizadas, y que se detecte y notifique oportunamente cualquier infracción de la seguridad. Se deben identificar las áreas críticas (áreas donde se almacena mercadería de exportación, zonas de carga o descarga, estacionamiento de camiones, playa de contenedores, sala de servidores, oficinas donde se encuentra la documentación de comercio exterior, etc.). Se deben analizar los flujos de mercaderías, vehículos y personas por estas áreas para determinar si es necesario eliminar o re direccionar los flujos que sean incompatibles como, por ejemplo, vehículos particulares en zonas de carga, acceso del personal a los vestuarios atravesando el área de despacho de mercadería, personas ajenas a la empresa transitando por oficinas de acceso restringido para acceder a baños o a una sala de reuniones, etc. Se debe realizar un análisis de las zonas vulnerables para impedir el acceso no autorizado a los locales de la organización (incluidas las oficinas, los almacenes y las instalaciones de embalaje), para garantizar que la información de la misma, los medios de transporte y la carga no sean manipulados o robados. Las organizaciones deben asegurarse de que estos locales cuenten con barreras físicas, elementos disuasorios que impidan el acceso no autorizado y los medios necesarios para garantizar una correcta vigilancia (iluminación, sensores, cámaras de video, etc.). Se debe prohibir que los vehículos de funcionarios o visitantes se estacionen en las zonas de manipulación y almacenamiento de la carga y los medios de transporte, o junto a ellos. Ubicar las áreas de estacionamiento fuera de las zonas valladas y/u operativas, o al menos, a una distancia considerable de las zonas de manipulación y almacenamiento de la carga. Las puertas por las que entren o salgan los vehículos y/o el personal (así como otros puntos de acceso, como las entradas a las instalaciones que no estén cerradas) deben estar vigiladas. Se recomienda que el número de puertas sea el mínimo necesario para el acceso y seguridad adecuados. En función del riesgo, las ventanas y puertas interiores y exteriores deben estar equipadas con dispositivos de cierre. Se debe definir en los procedimientos disposiciones que regulen cómo se disponen, cambian y retiran los dispositivos	•Procedimientos. • Plano de las instalaciones con áreas restringidas. •Plan de mantenimiento y reparación. •Registros de revisión, mantenimiento y reparación de infraestructura y sistemas, y otros registros que la organización implemente. •Constatación en recorrida por instalaciones.

		• Mantener los resultados documentados de estas inspecciones durante un tiempo suficiente para fines de auditoría. 15. Si el centro de monitoreo se encuentra tercerizado, tener procedimientos documentados que estipulen la funcionalidad de los sistemas críticos, los protocolos de autenticación para cambios de código de seguridad, altas o bajas del personal autorizado, revisión de contraseñas, acceso o denegación de acceso a sistemas, entre otros, en los contratos de servicio. 16. Revisar y actualizar los procedimientos de tecnologías de seguridad anualmente, o con mayor frecuencia dependiendo del nivel de riesgo. 17. Diseñar o instalar la tecnología de seguridad por personal calificado y debidamente acreditado. 18. Proteger físicamente la infraestructura de tecnología de seguridad contra accesos no autorizados. 19. Configurar los sistemas de tecnología de seguridad con una fuente de energía alternativa que permita que los sistemas continúen funcionando en caso de una pérdida inesperada de energía. 20. Instalar un sistema de cámaras de video vigilancia que permita monitorear las instalaciones y todas las áreas sensibles para impedir accesos no autorizados. 21. Colocar las cámaras para cubrir áreas clave de las instalaciones relacionadas con los procesos de embalaje, almacenamiento de las mercaderías, inspección de unidades de transporte e ITI, carga, descarga, precintado y desprecintado de las unidades de transporte e ITI. 22. Programar las cámaras para grabar con la configuración de calidad de imagen más alta razonablemente disponible, y configurar para grabar las 24 horas del día, los 7 días de la semana. El período de grabación recomendable es el tiempo que insuma el trayecto más largo del transporte de la mercadería a su destino final, más 14 días. 23. Mantener las grabaciones de las imágenes que cubren los procesos clave de importación/exportación/tránsito con el fin de permitir que se complete una investigación; teniendo en cuenta el período de tiempo recomendado en el numeral anterior. 24. Contar con una función de alarma/notificación en el sistema de cámaras que indique fallas en su funcionamiento o en la grabación. 25. Utilizar dichas alarmas para alertar a la organización sobre accesos no autorizados a las áreas sensibles. 26. Realizar revisiones periódicas y aleatorias de las imágenes de las cámaras (por parte de la gerencia, seguridad u otro personal designado) para verificar que los procedimientos de seguridad de la carga (seguridad de las unidades de transporte e ITI y seguridad de las mercaderías) se sigan correctamente. 27. Registrar los resultados de las revisiones para incluir cualquier acción correctiva tomada, y mantener durante un tiempo suficiente para fines de auditoría. 28. Asegurar la revisión periódica, el mantenimiento y la reparación de infraestructura, barreras físicas, equipos y sistemas empleados para la	de acceso, como las llaves. El retiro de los dispositivos de acceso debe tener lugar cuando los empleados cesen en la empresa. Una iluminación adecuada es un elemento de seguridad importante, tanto dentro como fuera de la instalación, incluyendo, según corresponda, las siguientes zonas: entradas y salidas, zonas de manipulación y almacenamiento de la carga, líneas de vallado y zonas de estacionamiento. Los temporizadores automáticos o los sensores de luz que encienden automáticamente las luces de seguridad son complementos útiles de los aparatos de iluminación. La tecnología de seguridad debe utilizarse para vigilar y asegurar/supervisar las áreas sensibles y los puntos de acceso. La misma incluye: sistemas de alarma antirrobo (perimetral e interior), también conocidos como Sistemas de Detección de Intrusos (SDI); dispositivos de control de acceso; y sistemas de video vigilancia (SVV), incluyendo cámaras de Circuito Cerrado de Televisión (CCTV). Un sistema CCTV/SVV puede incluir componentes como cámaras analógicas (coaxiales), cámaras basadas en el IP (basadas en la red), dispositivos de grabación y software de gestión de video. Las zonas seguras/sensibles dotadas de video vigilancia deben ser: las zonas de entrada y recepción de los edificios, las zonas de manipulación y almacenamiento de la carga, las zonas de envío/recepción en las que se guardan los documentos de comercio exterior, las salas en las que se almacenan los servidores de TI, las zonas de carga y almacenamiento de contenedores, las zonas en las que se inspeccionan los contenedores, y las zonas de almacenamiento de precintos. Las cámaras de video vigilancia son equipos que auxilian a la vigilancia y al registro, pero no son elementos de seguridad que por sí mismas eviten accesos no autorizados. Para asegurar su utilidad, es necesario contar con personal capacitado que sepa interpretar las imágenes y contar con un plan de revisión periódica de la calidad de los registros grabados y del campo de visión bajo distintas condiciones, para comprobar que no se hayan movido o que no haya elementos que impidan una buena visión como, por ejemplo, ramas de un árbol, suciedad, lluvia, vehículos estacionados, la posición del sol o de alguna lámpara, etc. El personal que opera y gestiona los sistemas tecnológicos de seguridad debe recibir formación o tener experiencia en operaciones y mantenimiento en sus áreas específicas. La infraestructura de tecnología de seguridad incluye computadoras, software de seguridad, paneles de control electrónico, video vigilancia o cámaras de CCTV,	

		seguridad de las instalaciones por el personal designado, conservando los registros correspondientes.	componentes de alimentación y disco duro para cámaras, así como grabaciones. Es importante contar con una fuente alternativa de energía para proteger la tecnología de seguridad en caso de sabotaje. Una fuente de energía alternativa puede ser una fuente de generación de energía auxiliar o baterías de respaldo. Los generadores de energía de respaldo también se pueden usar para otros sistemas críticos, como la iluminación. Es importante colocar las cámaras correctamente para permitir que las mismas registren tanto como sea posible el proceso de carga y descarga y de inspección y quienes intervienen en el mismo. Según el riesgo, las áreas o procesos clave pueden incluir el manejo y almacenamiento de carga; recepción del envío; el proceso de carga; el proceso de precintado; llegada/salida del transporte; servidores de TI; inspecciones de contenedores (de seguridad y agrícolas); almacenamiento de precintos; y cualquier otra área relacionada con la seguridad de los envíos internacionales. Una falla de los sistemas de video vigilancia podría ser el resultado de que alguien deshabilite el sistema para violar una cadena de suministro sin dejar evidencia en video del delito. La función de falla en el funcionamiento puede resultar en una notificación electrónica enviada a la persona designada previamente notificándole que el dispositivo requiere atención inmediata. Las cámaras no son solo herramientas de investigación, no se deben revisar solamente cuando se produce un incidente de seguridad. Si se usan de manera proactiva, pueden ayudar a evitar que ocurra una brecha de seguridad, realizando una revisión aleatoria de las imágenes para asegurarse de que la carga se mantuvo segura, y se siguieron todos los protocolos de seguridad. Algunos ejemplos de procesos que pueden ser revisados son los siguientes: actividades de manejo de carga; inspecciones de contenedores; el proceso de carga; el proceso de precintado; llegada/salida del medio de transporte; salida de la carga, etc. La revisión está destinada a evaluar el cumplimiento y la eficacia de los procedimientos de seguridad establecidos, identificar brechas o debilidades, y establecer acciones correctivas para mejorar los procesos de seguridad. Algunos de los elementos a incluir en el registro son: •la fecha de la revisión; •la fecha de la filmación que se revisó; •de qué cámara/área se realizó la grabación; •breve descripción de cualquier hallazgo; •si se justifica, acciones correctivas.	

			Todo edificio, planta o instalación debe inspeccionarse periódicamente en el marco de un programa global de mantenimiento. La inspección consiste en un recorrido a pie que permite al personal designado observar las instalaciones, evaluar la integridad de todos los elementos de seguridad (vallas, muros, puertas, ventanas, cerraduras, iluminación, alarmas, videocámaras sensores, etc.), recopilar información y anotar los elementos de interés. Lo ideal es que las inspecciones se programen, se completen cuando proceda y se documenten con un informe de resultados. Si se detectan daños, deben repararse lo antes posible. Asimismo, se deben tomar rápidamente medidas correctivas para eliminar cualquier condición peligrosa o brecha de seguridad.	

Todos los operadores	**4.5.8 Seguridad en el acceso de personas**	La organización debe: 1. Establecer procedimientos documentados que describan las medidas de seguridad para la identificación de los empleados, visitantes y contratistas, la confirmación de su identidad, y el control de acceso a las instalaciones. 2. Requerir a los visitantes y contratistas la presentación de una identificación con fotografía a su llegada, y mantener un registro que indique los detalles de la visita. 3. Entregar una identificación temporal a visitantes y contratistas, la que debe estar visible en todo momento durante la visita. 4. Acompañar a todos los visitantes y contratistas por personal designado. 5. Establecer y mantener procedimientos documentados para controlar y registrar la entrega, modificación, retiro, o eliminación de credenciales de identificación y de los dispositivos de accesos. 6. Definir e identificar las áreas de acceso restringido. El acceso a áreas sensibles debe estar restringido según la descripción del cargo o de las tareas asignadas. En las mismas se debe contar con los medios para reconocer accesos no autorizados. 7. Registrar el ingreso de visitantes y contratistas que acceden a las áreas críticas, de acuerdo al análisis de riesgo. 8. Incluir en los registros la siguiente información: • Fecha de la visita. • Nombre del visitante. • Empresa/institución. • Verificación de identificación con foto (documento de identidad). •Hora de llegada. • Punto de contacto de la empresa. • Hora de salida. Para los visitantes que concurren habitualmente se puede omitir la presentación de la identificación con foto, pero debe contarse con un listado actualizado de dichos visitantes, debiendo completarse igualmente la información requerida. 9. Registrar y verificar la identidad de los transportistas, acompañantes, verificadores, gestores u otras personas que tengan contacto con la carga, la documentación y/o los precintos de seguridad, previo a la recepción o entrega de la carga. 10. Requerir a los transportistas la presentación del documento de identidad o libreta de conducir para verificar su identidad. 11. Notificar, previo al arribo a las instalaciones, la hora estimada de llegada para el retiro programado de la carga, el nombre del conductor y los datos de la unidad de transporte. La organización debe permitir entregas y retiros de carga solo en los casos que fueran previamente coordinados. 12. Previo a su recepción, examinar los paquetes y el correo que llega periódicamente en busca de mercaderías no autorizadas. 13. Contar con procedimientos para identificar, enfrentar y retirar personas no autorizadas o no identificadas. El personal debe estar capacitado para responder a dicha situación, y conocer el procedimiento para su enfrentamiento y retiro.	El objetivo de la seguridad en el acceso de personas es evitar ingresos no autorizados a áreas críticas, manteniendo registro de las personas que ingresan y egresan. Los procedimientos de control y registro de accesos y el tipo de identificación utilizada, surgirán del análisis de riesgo. La aplicación de este requisito estará sujeta a las dimensiones de la empresa. No supone los mismos riesgos el ingreso a una oficina en la que trabajan 15 personas que el ingreso a una planta industrial con más de 100 empleados. El control de accesos debe diferenciar el tipo de registro e identificación utilizada para el personal de la empresa, visitantes que estarán acompañados y proveedores de servicios que podrían circular solos por distintas áreas de la empresa. Lo fundamental es que cualquier persona de la organización, no solamente los que tienen tareas específicas de vigilancia, puedan identificar fácilmente si una persona ajena se encuentra en un área restringida. Los visitantes, vendedores y proveedores de servicios deben presentar una identificación con fotografía a su llegada, y debe mantenerse un registro de los detalles de la visita. Además, todos los visitantes y proveedores de servicios deben recibir una identificación temporal la que debe estar visible en todo momento durante la visita. Con este fin son útiles tarjetas de identificación, chalecos, cascos o gorros de distintos colores. Los procedimientos deben establecer claramente cómo se regula la concesión, el cambio, el retiro y la eliminación de las tarjetas de identificación y de los dispositivos de acceso. Los dispositivos de acceso incluyen las tarjetas de identificación de los empleados, las tarjetas temporales de visitantes y proveedores, los sistemas de identificación biométrica, las tarjetas de proximidad, los códigos y las llaves. Cuando los empleados cesen su actividad en la empresa, el uso de listas de control de salida ayuda a garantizar que todos los dispositivos de acceso han sido devueltos y/o desactivados. En el caso de las empresas más pequeñas, en las que el personal se conoce entre sí y en función del riesgo, no se requiere ningún sistema de identificación. En los casos que visitantes frecuentes visiten las instalaciones deberán figurar en un listado como autorizados a ingresar sin presentación de documento oficial, pero igualmente se deberá registrar su ingreso y demás datos. Se debe mantener un registro de las personas que tengan contacto con la carga, la documentación y/o precintos de seguridad. En el caso de los transportistas, se debe registrar y verificar la identidad de los conductores solicitando un documento que acredite su identidad y los detalles del medio	• Procedimientos. •Registros de accesos de visitantes y contratistas. •Registro de credenciales o dispositivos de accesos. •Listado de visitantes o contratistas autorizados a ingresar. • Registro de transportistas y unidades de transporte. •Procedimiento o instrucciones de trabajo en caso de empresas tercerizadas de seguridad. •Otros registros que la organización implemente.

		14. Establecer procedimientos documentados con las instrucciones de trabajos para las tareas de los guardias de seguridad. 15. Verificar periódicamente el cumplimiento y la adecuación de estos procedimientos a través de auditorías y revisiones periódicas.	de transporte; dicha información debe ser validada con la información enviada previamente por la empresa transportista. Cuando los conductores llegan para recoger carga en una instalación de la organización se debe realizar el registro correspondiente. El registro debe contener la siguiente información: nombre del conductor; fecha y hora de llegada; empresa transportista; número de matrícula del tractor; número de matrícula del remolque; hora de salida; el número del precinto colocado en el momento de la salida, nombre del funcionario que registra, etc. Este criterio ayudará a las organizaciones a evitar que un transportista no autorizado retire carga (esquemas delictivos que resultan en el robo de carga). Una buena práctica es mantener una lista de los conductores con sus fotografías. Si no es factible saber de antemano qué conductor va a retirar la carga, la organización podrá verificar igualmente que el mismo esté aprobado para recoger la carga de la instalación. En lo relativo a revisión de paquetes y correo, los ejemplos de mercadería no autorizada incluyen, entre otros, explosivos, drogas, dinero. Se requiere establecer procedimientos para identificar y abordar a las personas no autorizadas/no identificadas y capacitar al personal sobre como reconocer y reportar estas situaciones. Si la organización contrata a una empresa de seguridad para que lleve a cabo el control de la seguridad de sus instalaciones, las tareas y actividades para ello deben estar documentadas en procedimientos o instructivos, se deben realizar capacitaciones a los guardias de seguridad para su correcta aplicación y verificar la eficacia del cumplimiento de los mismos.	

Todos los operadores	**4.5.9 Seguridad en la contratación del personal** **Contratación del personal**	La organización debe: 1) Establecer procedimientos documentados para definir el proceso de selección de personal, incluyendo las competencias requeridas del personal y la información a solicitar a los postulantes (datos personales, académicos, antecedentes y referencias laborales, referencias personales, etc.). 2) Verificar, previo a la contratación, la información brindada en la solicitud de aplicación al puesto de trabajo, el historial de empleo (CV) y las referencias personales, la identidad y los antecedentes laborales; tales resultados deben tenerse en cuenta a los efectos de la contratación. En áreas de mayor riesgo y puestos de mayor sensibilidad se pueden justificar investigaciones más profundas. 3) Realizar las verificaciones también para la contratación de trabajadores zafrales/eventuales y personal tercerizado, según la sensibilidad de los puestos de trabajo. 4) Realizar investigaciones periódicas basadas en causa justificada o según la sensibilidad del puesto de trabajo, luego de la contratación, atendiendo a la identificación de cambios inusuales en la situación social y económica de los empleados. 5) Controlar y mantener registros de la entrega de todos los elementos para el desarrollo de la actividad laboral, tales como uniformes, identificaciones, insignias, llaves, claves de acceso, cuentas de correo electrónico, usuarios de acceso a los sistemas, registro de firmas, autorizaciones o poderes para actuar en representación de la empresa, etc.	La organización debe contar con procedimientos y registros para: a) contratar al personal, b) sensibilizarlo respecto de los riesgos inherentes a la cadena logística de comercio exterior, c) capacitarlo en las tareas y responsabilidades que les competa en el marco del SGS, d) evaluar y dar seguimiento a su desempeño y conducta, e) y tomar las medidas necesarias en caso de desvinculación con la empresa. Previo a realizarse la contratación debe verificarse la información y los antecedentes; una vez realizada la misma debe considerarse la posibilidad de realizar nuevas investigaciones periódicas, o seguimiento en función de la sensibilidad del puesto del empleado, (principalmente aquellos puestos que implican acceso a información sensible, lugares o sistemas con implicancias de seguridad). Las causas de las nuevas investigaciones periódicas pueden surgir por: • reasignación, retención o promoción del empleado, • desempeño en el trabajo, • conflicto de intereses, • ausentismo inexplicable, •cambios inusuales en la situación social y económica aparente de un empleado.	•Procedimiento de selección y contratación de personal. •Planilla de trabajo MTSS. • Legajo de funcionario (donde se verifica que se cuente con un contrato de trabajo, alta BPS, CV, verificación de referencias aportadas por el solicitante). • Entrega de la política, evaluación de su entendimiento. • Inducción. •Contrato de confidencialidad de la información, si corresponde. • Registro de entrega de pertenencias para el desarrollo de sus tareas.

Todos los operadores	**Fortalecimiento del vínculo con el personal** **Finalización del vínculo laboral**	La organización debe: 6) Contar con políticas, estrategias o programas que promuevan el fortalecimiento del vínculo con el personal, basados en: a) el compromiso hacia las personas que trabajan en la organización, estando atento a circunstancias de su entorno social, familiar o económico que puedan requerir de apoyo y atención por parte de la organización; b) medidas que faciliten a los empleados plantear situaciones personales; c) un código de ética y conducta que establezca los principios y valores por los que se rigen; d) una definición clara de las medidas disciplinarias; e) una evaluación y seguimiento del desempeño y conducta de los empleados. 7) Evaluar periódicamente los resultados de las políticas, estrategias o programas establecidos. 8) Para los casos de desvinculación del personal controlar y mantener registros del retiro de todos los elementos otorgados, que puedan ser usados para afectar la seguridad de la misma, por ejemplo, uniformes, identificaciones, insignias, llaves, claves de acceso, cuentas de correo electrónico, usuarios de acceso a los sistemas, registro de firmas, autorizaciones o poderes para actuar en representación de la empresa, etc.	Cuando ocurren ilícitos dentro de las organizaciones en los que participa personal de la empresa es probable que hayan sido el resultado de circunstancias que involucran situaciones personales, familiares, económicas y sociales, por lo que se debe fortalecer el vínculo y el compromiso con los empleados, estando atento a circunstancias de su entorno que puedan requerir de apoyo y atención por parte de la organización. Se debe promover un vínculo de confianza que facilite a los empleados plantear situaciones personales, así como contar con personas capacitadas que sepan identificar indicios de estas situaciones para los casos en que la organización deba tomar la iniciativa. Charlas informativas, reuniones personales, actividades familiares dentro de la empresa son algunas de las prácticas recomendadas para abordar estos temas, así como contar con un código de ética y conducta, y establecer de forma clara las medidas disciplinarias. Las actividades de sensibilización, de capacitación o recreativas, plan de reuniones, etc. deben ser registradas, y los resultados pueden ser medidos mediante encuestas de satisfacción, rotación del personal, ausentismo, sugerencias de mejora realizadas por los empleados, y situaciones de apoyo personal en los que haya intervenido la organización. Esto último, como se trata casi siempre de situaciones delicadas, se mantiene en reserva por parte de los responsables de recursos humanos, pero un resumen general de lo actuado puede ser incluido por ejemplo en el informe de revisión por parte de la dirección. Los procedimientos escritos deben describir la sistemática a seguir para la desvinculación del personal, incluyendo el retiro de los dispositivos de acceso (llaves, tarjetas de identificación, etc.), así como otros elementos que podrían utilizarse para comprometer el acceso, como los uniformes.	• En la revisión por la dirección deberá evidenciarse el tratamiento de la gestión del personal, al menos con carácter general. • Registro de devolución de pertenencias y bajas de dispositivos de accesos a las instalaciones, y accesos informáticos.

Todos los operadores	**4.5.10 Seguridad de la Información**	La organización debe: 1) Establecer procedimientos documentados que expliciten las medidas de seguridad de la información, incluyendo los criterios de ciberseguridad para proteger los sistemas de Tecnología de la Información (TI). 2) Clasificar la información de acuerdo a su nivel de confidencialidad. 3) Establecer los niveles de acceso a la información y los controles de acceso, tanto del personal propio como del contratado, de los socios comerciales cuando corresponda, de acuerdo a las responsabilidades, a las funciones que desempeñan y al grado de confidencialidad de la información, de acuerdo a la clasificación realizada por la organización. 4) Establecer sistemas de cuentas y usuarios asignados individualmente para el personal con acceso a los sistemas de TI. Los accesos autorizados deben revisarse periódicamente para garantizar que el acceso a los sistemas sensibles se base en los requisitos y responsabilidades del cargo. 5) Eliminar el acceso a los dispositivos, a la red y a los sistemas al momento de la desvinculación del empleado. 6) Mantener un sistema para identificar accesos no autorizados a los sistemas/datos de TI, y para identificar el abuso de procedimientos, incluido el acceso inadecuado a sistemas internos o sitios web externos, la manipulación, alteración, copia, reproducción o extracción de información de la organización por parte de empleados o contratistas. Todos los infractores deben estar sujetos a las medidas disciplinarias correspondientes. 7) Proteger el acceso a los sistemas de TI contra la infiltración mediante el uso de contraseñas seguras, frases de contraseña u otras formas de autenticación; y debe protegerse el acceso de los usuarios a dichos sistemas de TI. 8) Establecer una sistemática de vigencia y renovación periódica de contraseñas. 9) Instalar suficiente protección software/hardware contra malware (virus, spyware, gusanos, troyanos, etc.) e intrusiones internas/externas (firewalls) en sus sistemas informáticos para defender los sistemas de TI contra las amenazas de ciberseguridad 10) Revisar los procedimientos de ciberseguridad anualmente, o con mayor frecuencia, según lo requieran los riesgos, las circunstancias o ante un incidente de seguridad, debiendo ser actualizados en caso de ser necesario. 11) Asegurar que su software de seguridad esté actualizado y reciba actualizaciones de seguridad periódicas. Si se encuentran vulnerabilidades, se deben implementar acciones correctivas tan pronto como sea posible. 12) Realizar copias de seguridad de los datos al menos una vez a la semana, o según corresponda. 13) Contabilizar a través de inventarios regulares todos los medios, hardware u otro equipo de TI que contengan información confidencial sobre los procesos operativos de la organización. 14) Almacenar los datos sensibles y confidenciales en un formato cifrado.	La ciberseguridad es la clave para salvaguardar los activos de la organización: la propiedad intelectual, la información de los clientes, los datos comerciales y financieros, los registros de los empleados, entre otros. Con una mayor conectividad a internet existe el riesgo de una violación de los sistemas de información de la organización. Esta amenaza puede afectar a organizaciones de todo tipo y tamaño. Las medidas para proteger la tecnología de la información (TI) y los datos son de vital importancia, y los criterios indicados proporcionan una base para un programa general de ciberseguridad para las organizaciones. Para la implementación se recomienda a modo orientativo la guía de requisitos que AGESIC entiende como necesario implementar para fortalecer la gestión de seguridad de la información, alineado con la normativa vigente y las mejores prácticas internacionales en la materia. Los requisitos detallados se encuentran asociados a las subcategorías del Marco de Ciberseguridad. Más información disponible en los siguientes enlaces: • https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion- • https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad/marco-ciberseguridad/nucleo-del-marcoconocimiento/comunicacion/publicaciones/guia-implementacion/guia-implementacion/requisitos • https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/guia-ciberseguridad-para-pequenas-empresas-emprendimientos/guia • https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad De acuerdo a las funciones y/o cargos, el personal debe recibir formación sobre las políticas y procedimientos de ciberseguridad de la organización. Esto debe incluir la necesidad de que los empleados protejan las contraseñas/frases de contraseña y el acceso a los dispositivos. El acceso a los sistemas informáticos debe estar protegido contra la infiltración mediante el uso de contraseñas sólidas, frases de contraseña u otras formas de autenticación, y el acceso de los usuarios a los sistemas informáticos debe estar protegido.	• Procedimiento. • Política de control de acceso lógico. • Política de gestión de usuarios y contraseñas. • Mecanismos de autenticación utilizados. • Esquema de seguridad de las aplicaciones críticas. • Listado de ingresos y egresos de funcionarios en el período auditado con detalle de su cargo y accesos otorgados o dados de baja (RRHH). • Solicitud de Alta/Baja de cuentas de usuario para acceso a equipos de red y comunicaciones, sistemas operativos, aplicativos, otros, para una muestra de funcionarios tomada del listado de ingresos y egresos obtenido de RRHH, para el período auditado. • Solicitud de modificaciones de privilegios de cuentas de usuario para acceso a equipos de comunicaciones, sistemas operativos, aplicativos y otros, dentro del período auditado. • Registro de verificación de sistemas.

		15) Limpiar de toda información y destruir adecuadamente los dispositivos, hardware u otro equipo de TI, de acuerdo con la normativa vigente en la materia. 16) Establecer procedimientos para prevenir ataques de ingeniería social. Si se produce una filtración de datos u otro evento inesperado que resulte en la pérdida de datos y/o equipos, los procedimientos deben incluir la recuperación (o reemplazo) de los sistemas y/o datos de TI. 17) Incluir en los procedimientos de ciberseguridad cómo la organización comparte información sobre amenazas de ciberseguridad con organismos estatales o socios comerciales. 18) Si se utilizan sistemas de red, probar periódicamente la seguridad de su infraestructura de TI. 19) Emplear tecnologías seguras, como redes privadas virtuales (VPN), para permitir que los empleados accedan a la intranet de la organización de forma segura cuando se encuentren fuera de la oficina, si es que la organización permite que sus usuarios se conecten de forma remota a la red. Si la organización permite que los empleados utilicen dispositivos personales para realizar el trabajo de la organización, todos estos dispositivos deben adherirse a los procedimientos de ciberseguridad para incluir actualizaciones de seguridad periódicas y un método para acceder de forma segura a la red de la organización. 20) Tener procedimientos diseñados para evitar el acceso remoto de usuarios no autorizados. 21) Incluir en los procedimientos de ciberseguridad medidas para prevenir el uso de productos tecnológicos falsificados o con licencia inadecuada. 22) Establecer sistemas que permitan asegurar la trazabilidad de las operaciones de comercio exterior. 23) Contar con un plan de continuidad del negocio frente a fallas de los sistemas informáticos, que incluya la modalidad de respaldo, almacenamiento y recuperación de la información y la protección de los equipos informáticos, especialmente los servidores.	Las contraseñas y/o frases de contraseña deben cambiarse lo antes posible si hay pruebas de que están en peligro, o haya sospechas razonables de tal peligro. Debe existir un sistema para identificar el acceso no autorizado a los sistemas/datos de TI o el abuso de las políticas y procedimientos, incluido el acceso indebido a los sistemas internos, o a los sitios web externos, y la manipulación o alteración de los datos de la organización por los empleados o contratistas. Debe haber una política o una lista de acceso que permita controlar el acceso físico a la sala de servidores de TI. Sólo el personal autorizado debe tener acceso a la misma. Una red segura es de suma importancia para una organización, y garantizar su protección requiere pruebas y verificaciones periódicas. Esto se puede hacer mediante la programación de escaneos de vulnerabilidad (VS) los que identifican puntos de entrada vulnerables en sus dispositivos (puertos abiertos y direcciones IP), sus sistemas operativos y el software a través del cual se podría obtener acceso a los sistemas de TI de la organización. El VS actúa comparando los resultados de su análisis con los de una base de datos de vulnerabilidades conocidas, y produce un informe de correcciones para que la organización tome medidas. La frecuencia de las pruebas dependerá de varios factores que incluyen el modelo de negocio y el nivel de riesgo de la organización. Por ejemplo, se deben realizar pruebas cada vez que hay cambios en la infraestructura de la red.	•Plan de recuperación y continuidad de negocio

Todos los operadores	**4.6 VERIFICACION Y EVALUACIÓN DE LA SEGURIDAD**	La organización debe evaluar sus planes, programas y competencias en la gestión de la seguridad, empleando para ello las revisiones, pruebas, ejercicios, informes de incidentes, evaluaciones de desempeño, etc., que entienda necesarias y adecuadas al análisis de riesgos.		• Procedimiento de incidentes, acciones correctivas y preventivas. • Procedimiento o protocolo de notificación de incidentes. Tener presente el instructivo DNA para la notificación de incidentes de seguridad: https://www.aduanas.gub.uy/innovaportal/file/21893/1/oec.it.08.v00-registro-de-un-incidente-de-seguridad-en-la-plataforma-web.pdf • Evidencia de implementación de alguna medida interna para notificaciones anónimas, buzón de sugerencias, aplicación informática, algún supervisor de RRHH, número de teléfono al que puedan denunciar.
	4.6.1 Incidentes, acciones preventivas y correctivas	La organización debe: 1) Establecer procedimientos documentados para registrar, reportar, investigar las causas de incidentes o fallos en el SGS (incluyendo falsas alarmas), definir e implementar las medidas correctivas que correspondan, registrar lo realizado (incluyendo las consecuentes modificaciones de los procedimientos involucrados), y verificar su eficacia. Se deberá incluir además el proceso de reporte en los distintos niveles jerárquicos. 2) Identificar la necesidad de implementar acciones preventivas. Las acciones preventivas deben contemplar al menos el análisis de riesgo realizado para planificar el SGS, los resultados de las evaluaciones realizadas al SGS, y un análisis de la evolución de los riesgos a nivel regional o internacional, así como de las modalidades delictivas que afectan el comercio internacional. 3) Contar con un procedimiento/protocolo de notificación para informar cualquier actividad sospechosa o incidente de seguridad que pueda afectar la seguridad de la cadena de suministro de la organización. 4) Informar los incidentes al Departamento OEC, a las autoridades pertinentes y a los socios comerciales que puedan ser parte de la cadena de suministro afectada. 5) Realizar las notificaciones a la DNA lo antes posible, y antes de que el medio de transporte o ITI involucrado cruce la frontera. 6) Incluir en su protocolo de notificación la información de contacto precisa, incluyendo nombre y números de teléfono del personal a notificar, así como de las autoridades pertinentes. 7) Revisar periódicamente el procedimiento/protocolo de notificación a efectos de mantener la información de contacto precisa y actualizada. 8) Establecer un mecanismo interno que permita a sus empleados informar de forma anónima asuntos relacionados con la seguridad, tales como conspiraciones internas, fraudes, robo, etc. Cuando se reciba dicha información, debe investigarse y tomar medidas correctivas, en caso de corresponder. 9) Iniciar un análisis posterior a la ocurrencia de un incidente de importancia que comprometa la seguridad de la cadena de suministro, inmediatamente después de tomar conocimiento de éste.	Los procedimientos para notificar incidentes de seguridad, actividades sospechosas y emergencias son aspectos extremadamente importantes de un programa de seguridad. La capacitación específica en función de los puestos de trabajo debe incluir los procedimientos de notificación, incluyendo aspectos específicos como qué notificar y a quién, cómo notificar un incidente y qué hacer una vez completada la notificación. Los problemas internos como robos, fraudes y conspiraciones internas pueden denunciarse más fácilmente si la parte denunciante sabe que lo puede realizar de forma anónima. La organización puede establecer un programa de línea directa o un mecanismo similar que permita a las personas permanecer en el anonimato si temen represalias por sus acciones. Se recomienda que cualquier informe se conserve como prueba para documentar que se investigó cada elemento informado, y que se tomaron medidas correctivas.	

Todos los operadores	**4.6.2 Análisis post incidente**	La organización debe: 1) Establecer un procedimiento documentado de análisis que incluya: a) los datos, documentos e información necesarios para determinar las causas del incidente; b) conocer dónde o quien tiene la vulnerabilidad en sus prácticas de seguridad; c) determinar dónde pudo haber estado comprometida la cadena de suministro; d) sistematizar la evidencia necesaria para deslindar responsabilidades. Dicho análisis no debe obstaculizar ni interferir con ninguna investigación de un organismo gubernamental con competencia en el asunto. 2) Documentar, finalizar tan pronto como sea posible y reportar al Departamento OEC, los resultados de la investigación posterior al incidente que efectúe la organización.	Se deberá establecer un análisis post incidente cuyo objetivo sea describir la metodología y la información necesaria para llevar a cabo la investigación, determinar si hubo fallas en el cumplimiento de los procedimientos del SGS de la organización, y/o su eventual responsabilidad. Se trata de un análisis en el que se establece qué datos, documentos e información son necesarios para determinar las causas de un incidente, y para conocer dónde está o quien tiene la vulnerabilidad en sus prácticas de seguridad. Una vez detectado el incidente la empresa establecerá las notificaciones correspondientes (Aduana, Dpto. OEC, etc.), y a partir del análisis realizado presentará las evidencias con las que cuenta tales como: • Análisis de riesgo. • Información de socios comerciales. • Cuestionarios y respuestas de los socios comerciales. • Procedimientos. • Documentación asociada a la operación de comercio exterior. • Registros de comunicaciones, correos, notificaciones. • Registros fílmicos y /o fotográficos. • Toda otra documentación que la organización entienda relevante para la investigación, o que solicite la DNA. En la plataforma de ingreso de Solicitudes OEC, se encuentra disponible una pestaña para el ingreso de incidentes y carga de la documentación respectiva; lo que deberá ser tenido en cuenta para su inclusión, tanto en el procedimiento de Incidentes como en el de comunicación de la organización.	• Registro del incidente y documentación asociada recopilada en el marco de la investigación, resultados y conclusiones.

Todos los operadores	**4.6.3** **Control de registros**	La organización debe: 1) Establecer un procedimiento documentado para controlar que los registros: a) estén accesibles para su utilización por parte del personal autorizado; b) estén debidamente identificados para evitar el uso de versiones obsoletas; c) sean fácilmente legibles; d) se almacenen adecuadamente y permanezcan protegidos contra daños, deterioro, pérdida o uso indebido; e) puedan recuperarse fácilmente durante su tiempo de conservación; f) se establezca, registre y respete su forma de disposición. 2) Mantener los registros necesarios para demostrar el cumplimiento de los requisitos OEC, los cuales deben incluir resultados de auditorías, mediciones, revisiones, evaluaciones, capacitaciones, etc.	Los registros permiten evidenciar las actividades ejecutadas para dar cumplimiento a los requisitos OEC y los resultados obtenidos. Asimismo, aportan datos e información para analizar el comportamiento y las mejoras de cada uno de los procesos del SGS. Los registros deben ser fácilmente identificables, estableciendo un formato y un campo identificador (nombre del registro, fecha de aprobación, código, versión, quien elabora, revisa, aprueba, etc.). Es necesario determinar dónde se realiza el archivo de los registros para poder encontrarlos fácilmente; el tiempo de conservación de los mismos; la metodología para acceder y encontrar registros de actividades anteriores; cómo se efectuará la eliminación de los registros o donde se archivarán de forma indefinida, si así se ha establecido. Se deben determinar los niveles de protección de los registros para así evitar cambios en la información que contienen, por ejemplo, protección con contraseña o con acceso restringido.	•Procedimiento de control de documentos. • Listado maestro de registros.
Todos los operadores	**4.6.4** **Auditorías**	La organización debe: 1) Establecer un procedimiento documentado de auditoría interna para verificar que el SGS es efectivo y funciona adecuadamente. 2) Establecer un programa de auditorías, ya sean estas generales o específicas, en el que se incluyan todos los requisitos OEC. 3) Controlar mediante las auditorías que el equipo y el personal de seguridad se desplieguen adecuadamente, identificar fortalezas, debilidades del SGS, oportunidades para la mejora, y verificar que la parte auditada de la organización realmente esté haciendo y logrando lo establecido en el SGS. 4) Documentar e informar a la dirección y a todo el personal pertinente las observaciones surgidas para que se establezcan las medidas para dar tratamiento e implementar las acciones requeridas. 5) Asegurar que los auditores que realicen las auditorías tengan las debidas competencias referentes a la seguridad en la cadena de suministro, ser conscientes de las implicancias de su rol, pudiendo ser personal propio de la organización, pero independiente de la actividad auditada.	El objetivo de una auditoría/revisión interna es garantizar que se cumplan los procedimientos por la organización. Las actividades de auditoría/revisión interna deben ser planificadas y realizarse regularmente, como mínimo una vez al año. La organización puede optar por realizar revisiones menores dirigidas a procedimientos específicos. Las áreas especializadas que son clave para la seguridad de la cadena de suministro, como las inspecciones y los controles de los precintos, pueden someterse a revisiones específicas. Sin embargo, es útil realizar periódicamente una revisión general para garantizar que todas las áreas funcionan según lo previsto. Las actividades de auditoría/revisión interna suelen ser realizadas por empleados de la organización de manera cruzada, asegurando la independencia de las actividades auditadas.	• Procedimiento de auditoría interna. • Programa de auditorías. • Informe de auditoría. • Registro que evidencie la comunicación de los resultados de la auditoría a la dirección y al personal. • Registro que evidencie el tratamiento de las observaciones. • Perfil de los auditores o CV.

Todos los operadores	**4.6.5 Revisión por la dirección**	La dirección de la organización debe: 1) Revisar, al menos una vez al año, el desempeño global y específico del SGS en base a la información que el propio sistema pone a su disposición. 2) Tomar como elementos de entrada el análisis de cada uno de los requisitos del Programa OEC, con el fin de determinar el desempeño y el nivel de cumplimiento de los mismos. 3) Documentar la revisión e incluir todas las decisiones y medidas tomadas en relación a posibles cambios en el SGS de la organización.	Para asegurar que el SGS es eficaz para la seguridad de la cadena de suministro, es necesario verificar que los procesos sigan siendo adecuados y que funcionan correctamente. La revisión debe incluir, al menos los siguientes elementos: a) el seguimiento del análisis de riesgo; b) el cumplimiento de los objetivos de seguridad y de los requisitos legales vigentes; c) la evaluación de los informes de las auditorías, las verificaciones y pruebas realizadas a los procedimientos; d) los registros de los incidentes de seguridad ocurridos desde la última revisión; e) los informes del estado de las acciones correctivas y preventivas; f) los resultados de los simulacros; g) la gestión de los recursos humanos, etc.; h) las circunstancias actuales de su negocio y de sus socios comerciales; i) los resultados de la medición y seguimiento del sistema; j) toda información adicional que se tenga en materia de seguridad. La revisión debe quedar documentada mediante un informe en el cual se incluya la información que se analizó al momento de la reunión, las decisiones tomadas y las acciones a realizar en relación a posibles cambios en el SGS y para la mejora continua del mismo (elementos de salida). En la reunión es conveniente la participación de la dirección o gerencia, del Representante OEC y de la persona encargada de la implementación y seguimiento del SGS, del grupo interdisciplinario y/o de los encargados de las áreas más relevantes.	• Se puede mencionar este requisito en el manual de seguridad o en un procedimiento. • Informe de revisión por la dirección.

Todos los operadores	**4.7 MEJORA CONTINUA**	La organización debe: 1) Implementar el SGS incluyendo dentro de la mejora continua todas las acciones realizadas para identificar, analizar, evaluar y tomar decisiones en las operaciones que realizan con miras a optimizar el desempeño de la organización. 2) Encomendar a los responsables de la implementación y mantenimiento del SGS los siguientes cometidos: a) el análisis y evaluación de la situación actual para identificar áreas y/o procesos para la mejora; b) el perfeccionamiento permanente de los procedimientos a los efectos de identificar acciones que permitan incrementar la efectividad en los procedimientos, y realizar adecuaciones para minimizar los errores o desviaciones que puedan detectarse; c) informar a la dirección sobre las acciones necesarias a implementar, y elaborar un programa en el que se establezcan las acciones de mejora, plazos, recursos y responsables para su ejecución (derivado de la revisión por la dirección); d) la medición, verificación, análisis y evaluación de los resultados de la implementación de dichas soluciones.	La organización debe tener un proceso para gestionar las actividades de mejora. Se deben identificar todos los procesos de la organización para analizarlos y buscar la forma de mejorarlos.	• Se puede mencionar este requisito en el manual de seguridad o en un procedimiento. • Registro, programa o plan en el que se identifiquen las áreas o procesos a mejorar, acciones de mejora, plazos, recursos, responsables y resultados de la evaluación de su implementación.

NOTAS:

CONSIDERACIONES GENERALES EN RELACIÓN A LOS REQUISITOS OEC - En la redacción de los Requisitos OEC se han integrado los enfoques que plantean:

- la Organización Mundial de Aduanas, a través de los lineamientos contenidos en el Marco Normativo SAFE, en la Guía Práctica para el Diseño e Implementación de un Programa de OEA en América Latina y en la Guía de implementación y Validación OEA 2021;
- los estándares CTPAT (Customs Trade Partnership Against Terrorism) de la Aduana de Estados Unidos (Customs and Border Protection - Homeland Security);
- la norma PU UNIT-ISO 28000 Especificaciones para los sistemas de gestión de la seguridad para la cadena de suministro.

Además de cumplir con sus correspondientes requisitos legales (Requisito OEC Nº 1), ser financieramente solvente (Requisito OEC Nº 2), contar con un historial de cumplimiento aduanero y tributario satisfactorio (Requisito OEC Nº 3), cada operador a certificarse o certificado OEC debe establecer y mantener un sistema de gestión de la seguridad (SGS) (Requisito OEC Nº 4). En este sentido, los requisitos del Programa OEC deben implementarse en base a un sistema de gestión que permita gestionar la seguridad de la carga en la cadena de suministro, controlar las amenazas y vulnerabilidades que pueden afectar la seguridad de la misma y, en caso de verse involucrado en un incidente de seguridad, permitir deslindar responsabilidades.

El Programa OEC contiene una estructura de requisitos adaptables a la realidad nacional y complejidad de los distintos operadores que participan del mismo, por lo que la implementación de los mismos dependerá del tamaño de la empresa, de la operativa y de las particularidades de cada modelo de negocio.

En el caso de las zonas francas que tengan por objeto la realización de actividades industriales, y en virtud del volumen de unidades de transporte que ingresan a diario a las plantas industriales a entregar el insumo principal de su proceso productivo, podrán implementar el requisito **4.5.3.3** prescindiendo del 100% de inspecciones de las unidades de transporte, en función de un análisis de riesgo que comprenda tanto el proceso operativo, como el de selección de sus proveedores de servicios de transporte nacional, ya sean contratados directamente o no por la organización. Para fortalecer la seguridad deben implementarse medidas alternativas de control.

MODIFICACIONES RESPECTO DE LA VERSIÓN ANTERIOR - Los cambios más significativos de esta nueva versión son los siguientes:

- Se simplifica la redacción y se reordena el requisito OEC N° 4 incorporando la gestión administrativa/documentación de comercio exterior al SGS.
- Se fortalecen todos los requisitos que hacen al SGS.
- Se incorporan nuevos conceptos fortaleciendo los criterios de seguridad en la cadena de suministro, tales como prevención de lavado de activos y financiamiento del terrorismo, instrumentos de tráfico internacional, seguridad agrícola, ciberseguridad.
- Se agrega al requisito sobre la política de seguridad la exigencia de referir explícitamente a los actos ilícitos en la cadena de suministro internacional como ser narcotráfico, contrabando, terrorismo, tráfico de productos falsificados, tráfico de armas, entre otros.
- Se incorpora la política contra el trabajo forzoso y trabajo infantil como parte de los valores de la empresa y del trabajo con sus socios comerciales, para no mantener relaciones comerciales con socios que estén vinculados a estos delitos.
- Se fortalece el requisito seguridad en las unidades de transporte de carga incorporando la seguridad de los Instrumentos de Tráfico Internacional - ITI.
- Se amplía el requisito sobre seguridad de los precintos incorporando la gestión, control y la metodología de verificación Ver/ Verificar/Tirar/Torcer (VVTT).
- Se incorpora un nuevo requisito sobre seguridad agrícola, con énfasis en el cumplimiento de la Norma Internacional para Medidas Fitosanitarias NIMF 15 de la Convención Internacional de Protección Fitosanitaria (CIPF): Reglamentación del embalaje de madera utilizado en el comercio internacional.
- Se jerarquiza la importancia de la gestión de los recursos humanos, así como también la capacitación en materia de seguridad.
- Se amplía el requisito de seguridad de la información incorporando conceptos de ciberseguridad.
- Se eliminan algunas redundancias.

EVIDENCIAS - Las evidencias que se indican en la columna final están establecidas de modo orientativo, la organización podrá implementar otros registros o documentos que den cuenta de la implementación de los requisitos, así como el Departamento OEC podrá solicitar evidencia complementaria para la validación de los mismos.