A. OBJETIVO

El objetivo de este documento es definir y describir los requisitos a ser cumplidos por parte de los operadores que aspiren a obtener y mantener la condición de Operador Económico Calificado (OEC).

B. CONSIDERACIONES GENERALES EN RELACION A LOS REQUISITOS OEC

Partiendo de la base de que las medidas de protección y seguridad deben estar presentes en todas las áreas de las empresas y considerando que el amplio espectro de operadores que integran la cadena de suministro internacional exige flexibilidad y adecuación a sus diferentes modelos de negocios, al elaborar los Requisitos OEC se han integrado, adaptándolos a nuestra realidad nacional, los enfoques que plantean:

- la Organización Mundial de Aduanas, a través de los lineamientos contenidos en el Marco Normativo SAFE y en las Guías Prácticas para el Diseño e Implementación de un Programa de OEC en América Latina,
- los estándares C-TPAT (Customs-Trade Partnership Against Terrorism) y
- la norma PU UNIT-ISO 28000:2007 Especificaciones para los sistemas de gestión de la seguridad para la cadena de suministro (versión diciembre 2008).

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) y con una adecuada gestión administrativa (Requisito OEC Nº 4), cada operador certificado o a certificarse OEC deberá establecer y mantener un Sistema de Gestión de la Seguridad (SGS) (Requisito OEC Nº 5) que incluya los siguientes aspectos esenciales:

5.1) Política de Seguridad,

5.2) Planificación de la Seguridad (análisis de riesgo, objetivos, indicadores y programas de seguridad),

5.3) Implementación y Operación de la Seguridad (responsabilidad y autoridad, toma de conciencia y competencias, comunicación, documentación, control de documentos, control operacional, preparación y respuesta ante emergencias),

5.4) Verificación de la Seguridad (medición y seguimiento, evaluación del sistema, incidentes y acciones preventivas y correctivas, control de registros y auditorías),

5.5) Revisión por la dirección,

5.6) Mejora Continua.

En base al contenido de este documento se ha elaborado el formulario de Autoevaluación OEC (OEC.RG.03), guía mediante la cual operadores que aspiren a

obtener la condición de OEC pueden determinar su grado de cumplimiento de los Requisitos OEC antes de presentar su Solicitud OEC (OEC.RG.02).

C. DEFINICIONES

Sistema de Gestión de la Seguridad (SGS): modo en que los operadores estructuran, organizan, documentan y llevan a cabo, sistemática y coordinadamente, sus actividades y prácticas de seguridad para, en base a su propio análisis de riesgos, prevenir, minimizar y controlar los riesgos a los que están sometidas sus operaciones de comercio exterior.

Socios Comerciales: se entiende por "socios comerciales" o por "asociados de negocios" a todos los terceros con los cuales un operador se vincula, comercial u operativamente, dentro de las cadenas de suministro internacional en las que participa. Incluye a sus clientes y a sus proveedores de productos (partes, materias primas y productos terminados) y de servicios de contratación directa y subcontratada (servicios administrativos y contables, transporte, almacenamiento de mercancías, tecnología, vigilancia, limpieza, etc.), ya sean éstos nacionales o extranjeros.

Crítico(a) en materia de seguridad: son aquellos componentes (instalaciones, equipos, productos, procesos, personas, etc.) propios de la organización o de sus socios comerciales, que por estar expuestos a amenazas con alta frecuencia y/o de gran incidencia y/o con bajo grado de control requieren que se establezcan medidas de prevención, control y minimización de su riesgo asociado.

D. REQUISITOS DEL OPERADOR ECONOMICO AUTORIZADO

REQUISITO OEC Nº 1 – Constitución Legal, Antigüedad y Cumplimiento de Normativa

La empresa debe estar legalmente constituida y tener una antigüedad mínima de 3 años en la realización de operaciones de comercio exterior. Debe contar con todas las autorizaciones que requieran la normativa nacional e internacional aplicable a sus operaciones, las cuales deben estar vigentes y disponibles para su comprobación por parte de la Dirección Nacional de Aduanas.

REQUISITO OEC Nº 2 – Solvencia Financiera

La empresa debe ser solvente al momento de presentar la Solicitud OEC, no pudiendo encontrarse en procesos de concurso, ser objeto de embargos judiciales ni estar sancionada mediante sentencia o resolución condenatoria en firme por falta de pago.

Se tomarán como indicadores en la evaluación de la solvencia las calificaciones de riesgo crediticio publicadas por el Banco Central del Uruguay y los ratios de liquidez de la empresa.

Si no hay entidades bancarias que califiquen a la empresa, la misma debe presentar al menos 4 referencias comerciales que certifiquen que operó internacionalmente sin inconvenientes financieros, cumpliendo regularmente con sus obligaciones de pago durante los tres últimos años.

La empresa debe cumplir con los requisitos establecidos por la Dirección General Impositiva en cuanto a la preparación y presentación de los estados contables.

REQUISITO OEC Nº 3 – Historial de cumplimiento aduanero y tributario

Presentar declaración jurada con un detalle de las causas en proceso o cerradas 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 este 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.

Tener, tanto la empresa, como sus propietarios y directores, un historial de cumplimiento aduanero y tributario satisfactorio, a juicio de la autoridad aduanera, de acuerdo a los criterios establecidos en las resoluciones que a sus efectos dicte la Dirección Nacional de Aduanas.

REQUISITO OEC Nº 4 – Gestión administrativa

La empresa debe tener procedimientos documentados y de aplicación comprobable para la gestión de comercio exterior (elaboración y presentación de documentos, seguimiento de los trámites aduaneros, etc.) y contar con un sistema contable actualizado y fiable para gestionar adecuadamente sus registros comerciales, garantizar su transparencia, mantenimiento, protección y accesibilidad para el control aduanero.

Debe contar, asimismo, con procedimientos, documentados y de aplicación comprobable para identificar, registrar y mantener actualizada la información considerada crítica en materia de seguridad de sus socios comerciales y productos comercializados (por ejemplo: productos sujetos a licencias y/o certificados, información financiera confidencial, etc.).

Se presentan a continuación requisitos aduaneros específicos por tipo de operador:

<u>Importadores/Exportadores</u>

- Oficina de comercio exterior físicamente definida, con personal afectado y funciones claramente establecidas.
- Archivo de 5 años de todas las operaciones de comercio exterior identificables por N° de DUA (Contenido de cada carpeta: factura definitiva, documentos de embarque, giros bancarios, flete y seguro, en caso de corresponder certificados de otros organismos (MSP, MGAP, etc.).
- En caso de realizar Admisiones Temporarias contar con: carpetas por N° de Admisión Temporaria (LATU), las afectaciones y el procedimiento de manejo de Stock.

Despachantes de Aduana

- Procedimiento establecido de preparación, liquidación y presentación del DUA ante la aduana.
- Procedimiento establecido de control de calidad previo a la presentación de los DUA ante la aduana.
- Procedimiento que defina las tareas que debe llevar a cabo el personal que interactúa con la Aduana y realiza el seguimiento de las operaciones con Observaciones pendientes.
- Procedimiento establecido para la presentación de PreGex y su seguimiento.
- Procedimiento establecido de seguridad de la información.
- Registros de antecedentes de los clientes que acrediten el conocimiento personal de los mismos, visitas a los domicilios constituidos declarados, por ejemplo: salones de venta, depósitos e instalaciones industriales.

Transportistas

- Oficina de Manifiestos definida físicamente, con personal afectado y funciones claramente establecidas.
- Procedimiento establecido para la confección de MIC/DTA o Manifiestos de Entrada /Salida y transmisión informática al Sistema LUCIA.
- Procedimiento que defina las tareas que debe llevar a cabo el personal que interactúa con la Aduana y realiza el seguimiento de las operaciones con Observaciones pendientes.
- Procedimiento establecido para la presentación de GEX y su seguimiento.
- Procedimiento establecido de seguridad de la información.
- Registros de antecedentes de los clientes que acrediten el conocimiento personal de los mismos, visitas a los domicilios constituidos declarados, por ejemplo: depósitos donde cargar o descargar mercadería.

- Archivo de 5 años de los MIC/DTA y Conocimientos de Embarque, identificables por N° de DUA.

Depositarios de mercadería en régimen suspensivo de derechos aduaneros

- Oficina de Control de Inventarios definida físicamente y con personal afectado y funciones claramente establecidas.
- Procedimiento establecido para la transmisión en tiempo real de los N° de Stock a la DNA.
- Procedimiento establecido para Vaciado/ Relleno de Contenedor, Fraccionamiento y Agrupamiento informático.
- Procedimiento que defina las tareas que debe llevar a cabo el personal que interactúa con la Aduana y realiza el seguimiento de las operaciones con Observaciones pendientes.
- Procedimiento establecido para poner la mercadería a disposición del Control Aduanero.
- Instalaciones apropiadas (físicas e informáticas) para el desarrollo de los controles aduaneros.

REQUISITO OEC Nº 5 – Sistema de Gestión de la Seguridad (SGS):

La empresa debe establecer, documentar, mantener y mejorar en forma continua un Sistema de Gestión de la Seguridad (SGS) que le resulte eficaz para identificar, tratar, controlar y minimizar las consecuencias de los riesgos de seguridad de su cadena de suministro internacional.

5.1 POLITICA DE SEGURIDAD

Por ser ésta una declaración en la que se establecen directrices globales en materia de seguridad debe: estar en consonancia con las demás políticas de la organización de los operadores certificados o a certificarse OEC, constituir el marco para el control de su operativa, manifestar su compromiso de cumplir la normativa nacional e internacional vigente y su voluntad de oponerse a todo acto o actividad ilícitos.

La Política de Seguridad debe estar documentada y ser puesta en conocimiento no sólo de la propia organización sino también de los socios comerciales pertinentes. La alta dirección debe validarla, respaldarla y promover su difusión y puesta en práctica.

5.2 PLANIFICACION DE LA SEGURIDAD

5.2.1 Análisis de Riesgo

Para que un SGS sea eficaz y eficiente debe ser planificado adecuadamente, en concordancia con el propio análisis de riesgo. El OEC, o quien desee certificarse como tal, debe establecer y mantener un procedimiento, documentado y de aplicación comprobable, para realizar un auto-análisis que le permita:

1) identificar los riesgos a los que están expuestos sus operaciones en particular y las cadenas de suministro en las que participa en general,

2) establecer el grado de control o la incidencia sobre cada riesgo identificado (*)

3) determinar la probabilidad de ocurrencia y la seriedad de las consecuencias de cada riesgo identificado y

4) establecer medidas de prevención y acciones de control adecuadas a cada riesgo analizado (*).

(*) Estos puntos requieren trabajar en cooperación con los socios comerciales.

El análisis de riesgo debe ser completo y comprender todos los componentes (instalaciones, equipos, productos, procesos, personas, información, etc.) que la organización defina como críticos en materia de seguridad (ver definición) de acuerdo a la naturaleza y a la escala del propio modelo empresarial.

Una vez al año como mínimo, o cuando se produzca una infracción o incidente de seguridad, el operador certificado o a certificarse OEC, debe revisar la metodología del análisis de riesgo para verificar su vigencia, aplicabilidad y eficacia.

5.2.2 Objetivos e Indicadores

Los objetivos de seguridad deben estar alineados a la política de seguridad, ser concretos, cuantificables y estar en conocimiento del personal propio y de los socios comerciales identificados como críticos en materia de seguridad.

Asimismo, cada área de la organización debe tener indicadores de seguridad (definidos a partir de los objetivos de seguridad) y una metodología definida para su medición y seguimiento.

Tanto los objetivos como los indicadores de seguridad deben revisarse y actualizarse periódicamente (con una frecuencia mínima anual) 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.

5.2.3 Programa de Seguridad

La organización debe contar con un programa de seguridad donde se establezcan los plazos, recursos y responsables para el logro de los objetivos de seguridad, así como los procedimientos, métodos y sistemas necesarios para realizarlo.

El programa de seguridad debe revisarse y actualizarse al menos una vez al año o cuando ocurra algún incidente de seguridad que amerite modificarlos.

5.3 IMPLEMENTACION Y OPERACIÓN DE LA SEGURIDAD

5.3.1 Responsabilidad y Autoridad

La organización debe tener claramente establecidas las responsabilidades y autoridades de todo su personal en relación a la seguridad.

La alta dirección debe involucrarse 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.

Debe haber una persona que, en calidad de representante de la dirección e independientemente de otras responsabilidades que tenga asignadas, sea responsable del funcionamiento del SGS (de su diseño, documentación, mantenimiento y mejora). Esta persona debe asegurar la complementariedad y coordinación de todos los programas de gestión de la seguridad de la organización, debe considerar y valorar los efectos adversos que la implementación de los mismos puede provocar en las distintas áreas de la organización y debe tener las potestades necesarias para garantizar el cumplimiento de todos los requisitos de seguridad aplicables a la organización y poner en práctica las medidas preventivas y correctivas que entiendan pertinentes a tales efectos.

5.3.2 Toma de Conciencia y Competencias

La organización debe establecer y mantener procedimientos para lograr que todas las personas involucradas en sus operaciones de comercio exterior tomen conciencia de la necesidad de respetar las normas de seguridad establecidas, de su incidencia en el logro de los objetivos de seguridad, de su propia responsabilidad sobre las personas, los procesos y los equipos que tienen a su cargo, de la importancia de aplicar correctamente los programas de seguridad establecidos y de las consecuencias que pueden provocar para la organización, en su conjunto, el incumplimiento de sus requerimientos en materia de seguridad.

En todos los niveles jerárquicos deben identificarse las competencias requeridas en materia de seguridad y la organización debe proporcionar la capacitación que corresponda al personal que no disponga de las mismas.

5.3.3 Comunicación

La organización debe establecer y mantener procedimientos para asegurar un intercambio fluido, abierto y efectivo de información relativa a la gestión de la seguridad de su cadena de suministro internacional, tanto con su propio personal y subcontratado como con todos sus socios comerciales críticos en materia de seguridad.

Nota: *en el manejo de la información se debe considerar la naturaleza confidencial de ciertos aspectos de la seguridad de la organización*.

5.3.4 Documentación

La documentación es necesaria para resguardar, fortalecer y mejorar el conocimiento que la organización tiene sobre su propio SGS. Para cumplir eficazmente estos cometidos debe ser clara, precisa y concisa.

La misma debe ser actualizada con regularidad (como mínimo anualmente), ser de fácil acceso y estar disponible para cada persona de la organización en la medida y con el grado de detalle que sus responsabilidades en materia de seguridad lo requieran.

La organización debe determinar el grado de confidencialidad de la documentación del SGS y su contenido debe comunicarse apropiadamente, tanto en la interna de la organización como a los socios comerciales (según el grado de responsabilidad correspondiente a cada involucrado).

La documentación del SGS debe incluir:

- la política y los objetivos de seguridad,
- la descripción de los elementos principales del SGS (manual de seguridad), su interrelación (incluyendo la referencia de los documentos asociados a cada elemento) y alcance,
- los documentos y los registros relativos a la planificación, implementación, operación y verificación de la seguridad, revisión por la dirección y mejora continua del SGS.

5.3.5 Control de Documentos

La organización debe establecer y mantener procedimientos, documentados y de aplicación comprobable para controlar todos los documentos relevantes de su SGS (ya sean de origen interno o externo) y:

- puedan ser localizados fácil y oportunamente,
- su contenido sea revisado y aprobado periódicamente por el personal autorizado a tales efectos,

- las versiones vigentes de los documentos correspondientes estén, disponibles y en buen estado de conservación, en todos los sitios en los que se los requiera para el eficaz funcionamiento del SGS,
- se evite el uso de versiones obsoletas de los mismos ,
- sean fácilmente identificables las versiones obsoletas que se conservan con el propósito de preservación legal o de conocimiento.

5.3.6 Control Operacional

5.3.6.A Seguridad en relación a los Socios Comerciales

La organización debe establecer y mantener procedimientos, documentados y de aplicación comprobable, para:

- La selección de socios comerciales confiables (tanto proveedores como clientes, ver definición)
- Verificar el emplazamiento de los socios comerciales (visita a las instalaciones de los socios comerciales críticos u otras medidas equivalentes que correspondan)
- Verificar los antecedentes de los socios comerciales críticos
- Registrar las certificaciones de SGS con las que cuentan los socios comerciales críticos en materia de seguridad
- En el caso de los socios comerciales que no cuentan con un SGS certificado, solicitar un compromiso formal de que cumplen con los Requisitos OEC que le sean aplicables y realizar auditorías periódicas para verificar su cumplimiento y actualizar el análisis de riesgo de la organización.

5.3.6.B Seguridad en las Unidades de Transporte de Carga

La organización debe establecer y mantener procedimientos, documentados y de aplicación comprobable, para:

- La inspección de las unidades de transporte de carga con criterios definidos de aceptación y rechazo y los puntos vulnerables a inspeccionar según el tipo de contenedor o unidad de transporte (Por ejemplo, paredes, piso, techo, cerrojos, bisagras, compartimientos ocultos en equipos de refrigeración, ruedas de repuesto, etc.)
- Registrar la inspección de las unidades de trasporte de carga
- Restringir el acceso a las áreas donde permanecen las unidades de transporte de carga durante la carga, espera o almacenamiento
- Verificar la identidad de los transportistas, acompañantes, verificadores, gestores u otras personas que tengan contacto con la carga, la documentación y los precintos de seguridad
- Asegurar que los precintos de seguridad utilizados en sus operaciones de comercio exterior cumplan la norma PAS ISO 17712 y que se mantienen en un

área de acceso restringido, se utilizan de forma aleatoria y se mantiene registro y control de los precintos utilizados y los disponibles
- Reconocer y denunciar la adulteración o uso fraudulento de los precintos de seguridad

5.3.6.C Seguridad en el Acceso de Personas

La organización debe establecer y mantener procedimientos, documentados y de aplicación comprobable, para:

- La identificación de los empleados, visitantes y contratistas
- Definir e identificar las áreas de acceso restringido. En las mismas se debe contar con los medios para reconocer accesos no autorizados
- Registrar el ingreso de visitantes y contratistas que acceden a las áreas críticas, coherente con el análisis de riesgo
- Identificar y retirar personas no autorizadas

Nota: *la aplicación de este requisito estará sujeta a las dimensiones de la empresa*.

5.3.6.D Seguridad en la Contratación del Personal

La organización debe establecer y mantener procedimientos, documentados y de aplicación comprobable, para:

- Definir las competencias requeridas del personal y la información a solicitar a los postulantes (datos personales, antecedentes laborales, académicos, referencias personales, etc.)
- Verificar los antecedentes de los postulantes
- Proporcionar inducción sobre el SGS, los requisitos de seguridad y sus responsabilidades a los nuevos empleados
- Sensibilizar periódicamente a los empleados y mantenerlos informados sobre la importancia de cumplir los requisitos de seguridad en la cadena logística y los riesgos de contrabando, narcotráfico, terrorismo, falsificaciones y otras actividades ilícitas asociadas al comercio internacional
- Capacitar al personal sobre cómo mantener la integridad de la carga y de los medios de transporte y cómo reconocer y reportar situaciones inusuales que puedan implicar conspiraciones internas, contaminación o alteración de la carga o de la documentación
- Identificar cambios inusuales en la situación social y económica de los empleados en posiciones críticas
- Controlar y mantener registros de la entrega y el retiro al personal de uniformes, identificaciones, insignias, llaves, claves de acceso, etc.

5.3.6.E Seguridad de las Mercaderías

La organización debe establecer y mantener procedimientos, documentados y de aplicación comprobable, para:

- Controlar y registrar las sucesivas etapas del movimiento de mercaderías (empaque, almacenamiento, carga, transporte, tiempos de tránsito en trayectos críticos, etc.)
- 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
- Controlar las mercaderías, su empaque, identificación y peso, definiéndose cómo investigar, notificar a responsables y autoridades y eventualmente solucionar discrepancias identificadas
- Registrar los procesos de carga que incluyan personal interviniente (responsable, datos del medio de transporte y del conductor, fotos o videos del estado de la carga y del sellado del vehículo o contenedor, etc.)
- Restringir el acceso a las áreas de empaque y carga de mercadería al personal autorizado y contar con una supervisión permanente durante estos procesos
- Controlar y registrar el uso de los materiales de empaque para evitar un uso indebido de los mismos (cajas, etiquetas, cintas con logo, etc.).

5.3.6.F Seguridad Físicas en las Instalaciones

La organización debe establecer y mantener procedimientos, documentados y de aplicación comprobable, para:

- Verificar y mantener la adecuación e integridad de las barreras físicas (como muros o cercos perimetrales), de las construcciones edilicias y sus materiales para impedir el acceso no autorizado a las instalaciones donde se manipula o almacena la carga
- Vigilar el acceso de vehículos y personas
- Identificar y separar las áreas de estacionamiento de vehículos privados de la de manejo, almacenaje y carga de mercadería
- Verificar que todas las ventanas y puertas de las áreas críticas cuenten con cerraduras.
- Registrar y controlar las llaves y tarjetas de acceso entregadas
- Iluminar externa e internamente las áreas críticas de modo que se puede realizar una vigilancia adecuada de las mismas
- Contar con sistemas de alarma y videocámaras acorde a la extensión y complejidad de las áreas a vigilar
- Restringir el acceso desde los vestuarios del personal a las áreas de almacenaje, acondicionamiento y carga
- Asegurar la revisión periódica y el mantenimiento (plan de mantenimiento y registros) de los cerramientos, cerraduras, iluminación y demás equipos y sistemas empleados para la seguridad de las instalaciones

5.3.6.G Seguridad de la Información

La organización debe establecer y mantener políticas, procedimientos y medidas de seguridad para el manejo de la información en sus sistemas informáticos. Los mismos deben estar documentados, ser de aplicación comprobable y comprender:

- la clasificación de la información según su grado de confidencialidad y los requerimientos para su protección
- los niveles de acceso a la información y los controles de acceso (del personal propio, el contratado y los socios comerciales) de acuerdo a sus responsabilidades y las funciones que desempeñan
- requisitos de seguridad para los socios comerciales que tienen acceso a sus sistemas informáticos
- la copia, reproducción o extracción de información de la organización
- los derechos de propiedad intelectual y de autor de los sistemas operativos y el software utilizado
- la trazabilidad de las operaciones de comercio exterior
- la protección de los sistemas informáticos frente a intromisiones en la red (antivirus, contraseñas que caduquen periódicamente, firewalls, servidores de autenticación, entre otros)
- el manejo y la protección de los equipos informáticos que procesan y almacenan información (especialmente los servidores)
- el resguardo histórico de la información (respaldo, almacenamiento y recuperación de la archivos)
- la identificación (sistema de detección y registro de incidentes de seguridad) y la penalización del abuso o la alteración de información crítica
- el mantenimiento y la reparación de los equipos informáticos
- el plan de continuidad del negocio frente a fallas de los sistemas informáticos

5.3.7 Preparación y Respuesta ante Emergencias

La organización debe establecer y mantener procedimientos y/o planes de contingencia, documentados y de aplicación comprobable, para actuar frente a las situaciones de emergencia identificadas en su propio análisis de riesgos, de modo de minimizar su impacto sobre la seguridad de las operaciones de comercio exterior y la empresa en su conjunto.

Cuando se evalúa la adecuación del SGS al análisis de riesgo (una vez al año, o cuando se produzca un incidente de seguridad, ver 5.2.1) debe verificarse también la vigencia, aplicabilidad y eficacia de los procedimientos y/o planes de contingencia.

Se deben realizar, asimismo, simulacros en los que se pongan a prueba los protocolos de actuación incluidos en los procedimientos de respuesta ante emergencias.

5.4 VERIFICACION DE LA SEGURIDAD

5.4.1 Evaluación del Sistema

La organización debe establecer y mantener procedimientos, documentados y de aplicación comprobable, para evaluar sus propios 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 a su propio análisis de riesgos.

Asimismo, debe evaluar el cumplimiento de la normativa vigente y comparar sus prácticas con respecto a las mejores prácticas de la industria a la que pertenece con una periodicidad apropiada para su escala y su propio modelo de negocios.

La organización debe llevar registro de los resultados de las evaluaciones que realice.

5.4.2 Incidentes y Acciones Preventivas y Correctivas

La organización debe establecer y mantener procedimientos, documentados y de aplicación comprobable, para: investigar las causas de incidentes o fallo 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.

La organización debe establecer y mantener procedimientos, documentados y de aplicación comprobable, para identificar la necesidad de implementar acciones preventivas. Las acciones preventivas deben contemplar al menos el análisis de riesgo realizado para planificar el SGS (5.2.1), los resultados de las evaluaciones realizadas al SGS (5.4.1) 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.

5.4.3 Control de Registros

La organización debe establecer y mantener procedimientos, documentados y de aplicación comprobable, para controlar que los registros de su SGS:

- estén accesibles para el personal autorizado a utilizarlos, debidamente identificados y sean fácilmente legibles
- se almacenen adecuadamente y permanezcan protegidos contra daños, deterioro, pérdida o uso indebido
- puedan recuperarse fácilmente durante sus tiempos de conservación correspondientes

- se establezca, registre y respete su forma de disposición

La organización debe llevar y mantener los registros necesarios para demostrar el cumplimiento de los Requisitos OEC, los cuales deben incluir resultados de auditorías, mediciones, revisiones, evaluaciones, capacitaciones, etc.

5.4.4 Auditorías

En forma adicional a la medición y el seguimiento rutinario del desempeño de su SGS (ver 5.4.1), la organización debe establecer y mantener un programa de auditorías, documentado y de aplicación comprobable, para verificar que dicho sistema sea efectivo y funcione adecuadamente, de modo que resulte útil para cumplir la política de seguridad y los objetivos de seguridad de la organización.

Los auditores que las realicen deben tener las debidas competencias y ser conscientes de las implicancias de su rol, aunque pueden ser personal propio de la organización, deben ser independientes de la actividad auditada.

El programa de auditorías debe basarse en el análisis de riesgo de la organización y en los resultados de las auditorías realizadas previamente.

Las auditorías, ya sean éstas generales o específicas, deben controlar que el equipo y el personal de seguridad se desplieguen adecuadamente, identificar fortalezas y debilidades del SGS y verificar que la parte auditada de la organización realmente esté haciendo y logrando lo que el sistema establece que haga y logre.

Los resultados de las auditorías deben ser informados a la dirección y a todo el personal pertinente para que se implementen las necesarias acciones requeridas.

5.5 REVISION POR LA DIRECCION

El diseño del SGS debe permitir que el mismo se adapte a los cambios internos y externos de la organización. La revisión por la dirección es una oportunidad para adecuarse a las circunstancias actuales del propio negocio y, de acuerdo a la visión de futuro de la dirección, tomar una postura proactiva de prevención y mejora en cuestiones de seguridad, especialmente en las áreas relativas vinculadas al comercio exterior.

La dirección de la organización debe revisar con una frecuencia establecida, el desempeño global y específico del SGS en base a la información que el propio sistema pone a su disposición (informes de las auditorías, resultados de la medición y seguimiento del sistema, registros de los incidentes de seguridad ocurridos desde la última revisión, informes del estado de las acciones correctivas y preventivas, cumplimiento de los objetivos de seguridad y de los requisitos legales vigentes, etc.), las circunstancias actuales de su negocio y toda información adicional que se tenga en materia de seguridad.

La revisión debe quedar documentada e incluir todas las decisiones y medidas tomadas en relación a posibles cambios en el SGS de la organización.

5.6 MEJORA CONTINUA

El SGS debe incluir la mejora continua en materia de control y prevención con el objetivo de incrementar el desarrollo y ejecución de actividades relativas a la seguridad de los procesos productivos y administrativos de la organización.

Los responsables del diseño e implementación del sistema deberían tener entre sus cometidos el perfeccionamiento permanente de los programas de seguridad, de modo que sus actividades regulares incluyan:

- el análisis y evaluación de la situación actual para identificar áreas y/o procesos para la mejora
- el establecimiento de objetivos para la mejora
- la búsqueda de posibles soluciones para lograr dichos objetivos
- la medición, verificación, análisis y evaluación de los resultados de la implementación de dichas soluciones.