

E10.

 <b>HACIENDA</b> <small>SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO</small>		 <b>SAT</b> <small>SERVICIO DE ADMINISTRACIÓN TRIBUTARIA</small>									
<b>Perfil de Parques Industriales</b>											
Primera Vez: <input type="checkbox"/>	Renovación: <input type="checkbox"/> <hr/> Adición: <input type="checkbox"/> Modificación: <input type="checkbox"/> Los datos que proporcione sustituirán los que proporcionó cuando solicitó su autorización.	Acuse de Recibo									
<p><b>Información General</b></p> <p>El objetivo de este Perfil, es el de asegurar que el parque industrial, desarrolle e implemente prácticas y procesos de seguridad que aseguren su cadena de suministro mitigando el riesgo de contaminación de sus instalaciones.</p> <p>Los parques industriales interesados en obtener la autorización a que se refiere la regla 7.1.5., deberán tener procesos documentados y verificables. Asimismo, que el industrial que se encuentre interesado en la autorización que se mencionó anteriormente deberá integrar los criterios exigidos en el presente documento al modelo o diseño empresarial que tenga establecido, buscando durante la implementación de los estándares en materia de seguridad la aplicación de una cultura de análisis que soporte la toma de decisiones acorde a los valores, misión, visión, códigos de ética y conducta de la propia empresa.</p> <p>Durante el llenado de este documento, los interesados en obtener la certificación analizarán e identificarán amenazas que les permitan implementar prácticas y procesos de seguridad que aseguren su cadena de suministros y minimicen el riesgo de contaminación o suplantación con mercancías ilícitas de las empresas que albergan.</p> <p><b>Instrucciones de llenado:</b></p> <p>I. Deberá llenar un "Perfil de Parques Industriales" por cada parque industrial, donde alberguen empresas que realicen operaciones de comercio exterior.</p> <p>II. Describir detalladamente cómo el parque industrial cumple o excede con lo establecido en cada uno de los numerales conforme a lo que se indica.</p> <p>III. El formato de este documento, se encuentra dividido en dos secciones, como se detalla a continuación:</p> <p style="margin-left: 40px;"><b>1. Estándar.</b></p> <p style="margin-left: 40px;">Descripción del estándar.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr style="background-color: #cccccc;"> <th colspan="2" style="text-align: left; padding: 5px;">1.1 Sub-estándar</th> </tr> <tr> <td colspan="2" style="padding: 5px;">Descripción del sub-estándar</td> </tr> <tr> <th style="width: 50%; padding: 5px;">Respuesta</th> <th style="width: 50%; padding: 5px;">Notas Explicativas</th> </tr> <tr> <td style="padding: 5px;"></td> <td style="padding: 5px;">                     Describa y/o anexe...                      a) Puntos a destacar...                 </td> </tr> </table>				1.1 Sub-estándar		Descripción del sub-estándar		Respuesta	Notas Explicativas		Describa y/o anexe... a) Puntos a destacar...
1.1 Sub-estándar											
Descripción del sub-estándar											
Respuesta	Notas Explicativas										
	Describa y/o anexe... a) Puntos a destacar...										

<b>IV.</b>	Indicar cómo cumple con lo establecido en cada uno de los sub-estándares, por lo que deberá anexar los procedimientos en idioma español, estos procedimientos deben caracterizarse por describir o definir el objetivo que persigue el documento, el inicio y fin del proceso, indicadores de medición, requisitos, documentos o formatos a utilizar, responsables, por mencionar algunos. El apartado referente a las “ <b>Notas Explicativas</b> ” es una guía respecto a los puntos que se deben incluir en la “ <b>Respuesta</b> ” de cada sub-estándar, señalando de manera indicativa aquellos puntos que no deben excluirse de su respuesta.		
<b>V.</b>	Una vez contestado este “Perfil de Parques Industriales”, deberá anexarlo a la Solicitud de inscripción en el registro de Socio Comercial Certificado a que se refiere el primer párrafo de la regla 7.1.5., fracción IV, inciso a).		
<b>VI.</b>	Para efectos de verificar lo manifestado en el párrafo anterior, el SAT a través de la AGACE, podrá realizar una inspección a la instalación aquí señalada, con el exclusivo propósito de verificar lo señalado en este documento.		
<b>VII.</b>	Cualquier “Perfil de Parques Industriales” incompleto no será procesado.		
<b>VIII.</b>	Cualquier pregunta relativa a la Solicitud de inscripción en el registro de empresas certificadas y al “Perfil de Parques Industriales”, dirigirla a los contactos que aparecen en el Portal del SAT.		
<b>IX.</b>	En el caso de ser autorizado como Socio Comercial Certificado, este formato deberá mantenerse actualizado y dar aviso cuando las circunstancias por las cuales se les otorgó el registro hayan variado y derivado de estas se requieran cambios o modificaciones en la información vertida y proporcionada en este “Perfil de Parques Industriales” a la autoridad, de conformidad con lo establecido en la regla 7.2.1., cuarto párrafo, fracciones I, II y VII.		
<b>X.</b>	Cuando derivado de la visita de inspección resulten incumplimientos relacionados con los estándares mínimos en materia de seguridad, la solicitante podrá subsanarlos antes de la emisión de la resolución establecida en la regla 7.1.6., para lo cual tendrá un plazo máximo de tres meses contados a partir de la notificación de los incumplimientos señalados.		
<b>Datos de la instalación</b>			
Se deberá llenar un “Perfil de Parques Industriales” por cada una de las instalaciones que pertenezcan y operen bajo el mismo RFC y que realicen procesos de manufactura de productos objeto de comercio exterior, y en su caso, de aquellas instalaciones relacionadas como plantas industriales y/o manufactureras, almacenes, centros de distribución, consolidación, etcétera.			
<b>Información de la Instalación</b>	<b>Número de “Perfil de Parques Industriales”:</b> _____ de _____		
Clave en el RFC	Nombre y/o Razón Social:		
Nombre y/o Denominación de la Instalación			
Tipo de Instalación			
Calle	Número y/o letra exterior	Número y/o letra interior	
Colonia	Código Postal	Municipio/Delegación	Entidad Federativa
Antigüedad de la instalación (años de operación)		Actividad preponderante	
No. de empleados total de esta instalación:		Superficie de la instalación (M <sup>2</sup> ):	

<b>Certificaciones:</b> (indicar si cuenta con certificaciones que consideren que impactan en el proceso de su cadena de suministros, por ejemplo: ISO 9000; Procesos Logísticos Confiables, entre otros)		
Nombre: _____	Categoría: _____	Vigencia: _____
Nombre: _____	Categoría: _____	Vigencia: _____
Nombre: _____	Categoría: _____	Vigencia: _____
Nombre: _____	Categoría: _____	Vigencia: _____
<b>1. Planeación de la seguridad en la cadena de suministros.</b>		
<p>El Parque Industrial debe elaborar políticas y procedimientos documentados para llevar a cabo un análisis que le permita identificar riesgos y debilidades en las instalaciones con el objetivo de que el Corporativo, implemente estrategias que ayuden a mitigar, los riesgos en el Parque Industrial.</p> <p>Asimismo, para construir un programa sólido de seguridad de la cadena de suministro, la empresa debe de contar con un Comité de Seguridad que incorpore representantes de todos los departamentos relevantes, formando un equipo multifuncional que identifique áreas de oportunidad y proponga acciones de mejora continua a lo largo de la cadena de suministro e instalaciones de la compañía.</p> <p>De igual manera, la empresa debe tener designados puntos de contacto para el Programa Operador Económico Autorizado, dicho personal debe involucrarse, conocer los requisitos del programa, pertenecer a la compañía y acreditar su relación con la misma, así como responder a su especialista en seguridad de la cadena de suministro.</p> <p>Si derivado del análisis de riesgo, surgen nuevas medidas de seguridad para incorporarse dentro del parque industrial, estas deben incluirse en los procedimientos existentes de la empresa y, en su caso, elaborar procedimientos nuevos, lo que crea una estructura más sostenible y enfatiza que la seguridad de la cadena de suministro es responsabilidad de todos.</p>		
<b>1.1 Análisis de riesgo.</b>		
<p>Los parques industriales deben establecer medidas para identificar, analizar y mitigar los riesgos de seguridad al interior de sus instalaciones, particularmente en las áreas que son de uso común o compartido por las empresas domiciliadas en su interior. Por tal motivo, se debe desarrollar un análisis por escrito para determinar riesgos con base en el modelo de su organización (ejemplo: ubicación geográfica, índice delictivo, actividad preponderante de las empresas copropietarias y/o arrendatarias, tipo de mercancía, peligrosa, alto valor, etcétera), que le permita implementar y mantener medidas de seguridad apropiadas. Conforme a lo anterior, también debe tener un proceso escrito basado en su análisis de riesgo para seleccionar nuevos socios comerciales y monitorear a los socios con los que ya se encuentra trabajando.</p> <p>Este procedimiento debe actualizarse por lo menos una vez año, de manera que permita identificar otros riesgos o amenazas en las instalaciones del Parque, por el resultado de algún incidente de seguridad o que se originen por cambios de las condiciones iniciales en la operación, así como para identificar que las políticas, procedimientos y otros mecanismos de control y de seguridad se estén cumpliendo. Es importante señalar, que el Comité de Seguridad de la compañía debe de participar en la elaboración y actualización del análisis de riesgo y el mantenimiento del Programa Operador Económico Autorizado.</p>		

Respuesta:	Notas Explicativas:
	<p>Indicar cuáles son las fuentes de información utilizadas para calificar los riesgos durante la fase de análisis.</p> <p>Anexar la matriz de riesgos, así como el procedimiento documentado para identificar riesgos en las instalaciones del Parque Industrial, el cual debe incluir como mínimo los siguientes puntos:</p> <ol style="list-style-type: none"> <li>I. Periodicidad con que revisa y/o actualiza el análisis de riesgo.</li> <li>II. Áreas y/o empresas del Parque Industrial que se incorporan al análisis de riesgo.</li> <li>III. Metodología o técnicas utilizadas para realizar el análisis de riesgo.</li> <li>IV. Responsables de revisar y/o actualizar el análisis de riesgo de la empresa.</li> </ol> <p>Asimismo, el procedimiento documentado para identificar riesgos en la cadena de suministro y sus instalaciones, deberá contemplar el proceso de apreciación y gestión del riesgo, e incluir los siguientes aspectos:</p> <ol style="list-style-type: none"> <li>I. Establecimiento de un contexto (cultural, político, legal, económico, geográfico, social, etcétera).</li> <li>II. Identificación de los riesgos en su cadena de suministros y sus instalaciones.</li> <li>III. Análisis del riesgo (causas, consecuencias, probabilidades y controles existentes para determinar el nivel de riesgo como "alto", "medio" y "bajo").</li> <li>IV. Evaluación del riesgo (toma de decisiones para determinar los riesgos a tratar y prioridad para implementar el tratamiento).</li> <li>V. Tratamiento del riesgo (aplicación de alternativas para cambiar la probabilidad de que los riesgos ocurran).</li> <li>VI. Seguimiento y revisión del riesgo (monitoreo de los resultados del análisis de riesgo y verificación de la eficacia de su tratamiento).</li> </ol> <p>Se sugiere utilizar las técnicas de administración, gestión y de evaluación de riesgos de acuerdo a las normas internacionales ISO 31000, 31010 e ISO 28000 que, de acuerdo a su modelo de negocio, deban implementar.</p>

<b>1.2 Políticas de seguridad.</b>	
<p>Los parques industriales deben contar con una política orientada a prevenir, asegurar y reconocer amenazas en la cadena de suministros, e instalaciones de la compañía, como lo son el tráfico de drogas, lavado de dinero, tráfico de armas, contrabando de personas, mercancías prohibidas y actos de terrorismo. Por su parte, las empresas copropietarias y/o arrendatarias que operan en el parque industrial, deben suscribir y cumplir su política de seguridad. Lo anterior, independientemente de que algunas empresas no realicen operaciones de comercio exterior o que ya estén certificadas en materia de seguridad en la cadena de suministros.</p> <p>Para promover una cultura de seguridad, las compañías deben demostrar su compromiso con la seguridad de la cadena de suministro y el Programa Operador Económico Autorizado a través de una declaración que resalte la importancia de proteger el flujo del comercio nacional e internacional de actividades delictivas, establecida por medio de la política de seguridad.</p> <p>Los altos funcionarios o directivos de la empresa que deben respaldar y firmar la política de seguridad pueden incluir al presidente de la compañía, al director ejecutivo, al gerente general, al director de seguridad o personal con cargo homólogo con facultad para toma de decisiones.</p>	
<b>Respuesta:</b>	<b>Notas Explicativas:</b>
	<p>Enunciar la política de seguridad orientada a prevenir, asegurar y reconocer amenazas en la cadena de suministros e instalaciones de la compañía, indique quién es el responsable de su revisión, firma y difusión hacia los empleados, así como la periodicidad con la que se lleva a cabo su actualización.</p> <p>Dicha política se debe comunicar a los empleados mediante un programa y/o campaña de difusión.</p> <p>La política de seguridad debe estar firmada por un alto funcionario de la compañía y estar exhibida en diversas áreas de la empresa, incluyendo el sitio web de la empresa, carteles en áreas clave de la empresa (recepción, embarques, recibos, almacén, etcétera), y como parte de la capacitación inicial y de reforzamiento de la empresa.</p> <p>Deberá tener registros de la política de seguridad firmada por las empresas copropietarias y/o arrendatarias que operan de conocimiento y aceptación.</p>
<b>1.3 Auditorías internas en la cadena de suministros.</b>	
<p>Además del monitoreo y la supervisión de rutina en los controles de seguridad, es necesario programar y realizar auditorías periódicas, que permitan evaluar todos los procesos en materia de seguridad en la cadena de suministros de una manera más crítica y profunda, así como garantizar que sus empleados sigan los procedimientos de seguridad de la empresa.</p> <p>Las auditorías deben ser realizadas por el Comité de Seguridad de la compañía, establecer un procedimiento documentado, así como un programa o calendario para su realización. Si bien es necesario que las auditorías estén enfocadas en la seguridad de la cadena de suministro y basadas en la evaluación, revisión y ejecución de los estándares mínimos en materia de seguridad, su enfoque se debe ajustar al tamaño de la organización, nivel a la naturaleza de riesgos, modelo de negocio y variaciones entre instalaciones. Las auditorías pueden ser generales o centrarse en áreas o procesos específicos conforme a su programa de trabajo.</p> <p>El objetivo de una auditoría interna enfocada al Programa Operador Económico Autorizado, es verificar y garantizar que los empleados sigan los procedimientos de seguridad de la empresa. El proceso de revisión no tiene que ser complejo, sin embargo, los formatos y registros que se utilicen para la aplicación de dichas revisiones deben de evidenciar que se validó la aplicación y ejecución de los procesos evaluados, además del seguimiento correspondiente de las observaciones identificadas.</p> <p>La alta gerencia del Corporativo del Parque Industrial debe revisar los resultados de las auditorías, y emprender las acciones correctivas o preventivas requeridas. El proceso de auditoría debe garantizar que se recoja la información necesaria para permitir que la gerencia realice está evaluación. La revisión debe estar documentada, además de que el Comité de Seguridad de la empresa deben proporcionar y registrar las actualizaciones periódicas sobre el progreso o los resultados de cualquier auditoría, ejercicio o validación.</p>	

Respuesta:	Notas Explicativas:
	<p>Describir el procedimiento documentado para llevar a cabo una auditoría interna, enfocada en la seguridad de la cadena de suministros, asegúrese de incluir los siguientes puntos:</p> <ol style="list-style-type: none"> <li>I. Señalar cómo la empresa lleva a cabo la programación o calendarización para realizar una auditoría interna en materia de seguridad, en la cadena de suministros y seguridad de las instalaciones.</li> <li>II. Indicar quienes participan en ellas, y los registros que se efectúan del mismo, así como periodicidad con la que se llevan a cabo.</li> <li>III. Indicar cómo es que la gerencia del Corporativo del Parque Industrial verifica el resultado de las auditorías en materia de seguridad, cómo realiza y/o implementa acciones preventivas, correctivas y de mejora, además del seguimiento y cierre de las mismas.</li> <li>IV. Los formatos utilizados durante las auditorías internas deberán de estar debidamente requisitados, y a través de ellos, evidenciar que los procedimientos y medidas de seguridad se están poniendo en práctica.</li> </ol>
<p><b>1.4 Planes de contingencia y/o emergencia.</b></p>	
<p>Debe existir un plan de contingencia y/o emergencia documentado, dicho plan debe abordar la gestión de crisis, los planes de recuperación de la seguridad y la reanudación del negocio, para asegurar la continuidad del negocio en caso de una situación que afecte el desarrollo normal de las actividades y las operaciones de comercio exterior del parque industrial en su cadena de suministros. Una crisis o contingencia puede incluir la interrupción del movimiento de datos comerciales debido a un ataque cibernético, un incendio, una amenaza de bomba, la detección de paquetes sospechosos, el corte de energía eléctrica, el robo y/o daño de mercancías, (Por ejemplo: bloqueos carreteros, de vialidades internas, vialidades urbanas, tiroteos, amenazas, o extorsiones, ingreso de personal no autorizado, daño de instalaciones, entre otros, cierre de aduanas).</p> <p>Dichos planes deben ser comunicados al personal del parque industrial, como a los responsables de seguridad de las empresas establecidas en el mismo, mediante capacitaciones periódicas, así como realizar pruebas, ejercicios prácticos y simulacros anuales de los planes de contingencia y emergencia para constatar su efectividad, mismos de los que deberá mantener un registro debidamente requisitado y firmado (por ejemplo: reportes de resultados, minutas o informes, los cuales deberán ir respaldados de videgrabaciones, fotografías, etcétera, que demuestren su ejecución).</p> <p>El plan de contingencia y/o emergencia debe actualizarse según sea necesario, en función de los cambios en las operaciones y el nivel de riesgo de la organización.</p>	

Respuesta:	Notas Explicativas:
	<p>Anexar el procedimiento o plan de contingencia y/o emergencia documentado, para asegurar la continuidad del negocio en caso de una situación de emergencia o de seguridad, que afecte el desarrollo normal de las actividades de comercio exterior empresas instaladas en el parque industrial.</p> <p>Este procedimiento debe incluir, de manera enunciativa mas no limitativa, lo siguiente:</p> <ol style="list-style-type: none"> <li>I. Qué situaciones contempla, describiendo el plan de acción y pasos que hay que seguir en caso de crisis, así como las tareas que el personal tenga asignadas durante el manejo de dichas contingencias.</li> <li>II. Qué mecanismos utiliza para difundir y asegurarse que estos planes sean efectivos.</li> <li>III. Contemplar la programación y realización de simulacros anuales y cómo se documentan (por ejemplo: reportes de resultados, minutas o informes, mismos que deberán ir acompañados de videograbaciones, fotografías, etcétera, que demuestren su ejecución).</li> </ol>
<b>2. Seguridad física.</b>	
<p>El parque industrial debe contar con mecanismos y procesos documentados para impedir, detectar o disuadir la entrada de personal no autorizado a las instalaciones. Todas las áreas deben tener barreras físicas, elementos de control y disuasión contra accesos no autorizados.</p>	
<b>2.1 Instalaciones.</b>	
<p>Las instalaciones (oficinas administrativas, naves industriales, almacenes, etcétera) deben estar construidas con materiales que puedan resistir accesos no autorizados. Se deben realizar inspecciones periódicas documentadas para mantener la integridad de las estructuras y en el caso de haber detectado una irregularidad, efectuar la reparación correspondiente y lo antes posible por parte del personal designado para estas tareas. Asimismo, se deben tener identificados plenamente los límites territoriales, así como los diversos accesos, vialidades internas, externas y la ubicación de edificios administrativos, naves industriales, almacenes, áreas de estacionamiento para vehículos de empleados y de carga, predios baldíos, espuelas de ferrocarril y proyectos de ampliación a corto o mediano plazo.</p>	

Respuesta:	Notas Explicativas:
	<p>Indicar los materiales predominantes con los que se encuentran construidas las instalaciones (por ejemplo, estructura metálica, paredes de lámina, paredes de ladrillo, concreto, malla ciclónica, entre otros), y señale de qué forma se lleva a cabo la revisión y mantenimiento de la integridad de las estructuras.</p> <p>Indicar el personal o área responsable para realizar las tareas de inspección, mantenimiento y reparación de daños de las instalaciones.</p> <p>Anexar un plano de distribución o arquitectónico del conjunto, donde se puedan identificar los límites, rutas de acceso, de las instalaciones, la ubicación de los inmuebles, áreas críticas, estacionamiento y colindancias.</p> <p>En el supuesto de que dos propietarios o inquilinos del Parque Industrial realicen operaciones de comercio exterior y compartan un Almacén o patio de maniobras para vehículos de carga, debe señalarlo en el Plano arquitectónico de conjunto.</p>
<b>2.2 Accesos en puertas y casetas.</b>	
Las puertas de entrada o salida de vehículos y/o personal deben ser atendidas, controladas, vigiladas y/o supervisadas. La cantidad de puertas de acceso debe mantenerse al mínimo necesario. El acceso a las áreas sensibles debe estar restringido según la descripción del trabajo o las tareas asignadas.	
Respuesta:	Notas Explicativas:
	<p>Indicar cuantas puertas y/o accesos (peatonales, autos particulares, vehículos de carga, espuela de ferrocarril) existen en el parque industrial, así como el horario de operación de cada una, e indique de qué forma son monitoreadas (Debe tener personal de seguridad e indicar la cantidad de elementos).</p> <p>Detallar si existen puertas y/o accesos bloqueos o permanentemente cerrados.</p> <p>Describir cómo asegura que el acceso a las áreas sensibles este restringido según la descripción del trabajo o las tareas asignadas (incluya el tipo de registros y controles que utiliza).</p>

<b>2.3 Bardas perimetrales.</b>	
<p>Las bardas perimetrales, deben instalarse para asegurar los perímetros del parque industrial, con base en un análisis de riesgo realizado por el corporativo. Se deben utilizar cercas que permitan impedir y disuadir intrusiones al parque industrial. Estas deben ser inspeccionadas regularmente y llevar un registro de la revisión con la finalidad de asegurar su integridad e identificar daños, mismos que deben repararse lo antes posible por parte del personal designado para estas tareas.</p>	
<b>Respuesta:</b>	<b>Notas Explicativas:</b>
	<p>Describir el tipo de cerca, barrera periférica y/o bardas con las que cuenta el parque industrial, asegúrese de incluir los siguientes puntos:</p> <ol style="list-style-type: none"> <li>I. Especificar qué áreas encierra.</li> <li>II. Señalar las características de las mismas (material, dimensiones, etcétera).</li> <li>III. En caso de no contar con bardas, justificar detalladamente la razón y explicar cómo subsana esta situación.</li> <li>IV. Periodicidad con la que se verifica la integridad de las bardas perimétricas y los registros que se llevan a cabo, con la finalidad de asegurar su integridad e identificar daños, mismos que deben repararse lo antes posible.</li> <li>V. Indicar el personal o área responsable para realizar las tareas de inspección y reparación de daños.</li> <li>VI. Identificar y señalar las áreas de acceso restringido.</li> </ol> <p>El procedimiento para la inspección de las bardas perimétricas podría incluir:</p> <ol style="list-style-type: none"> <li>I. Personal responsable para llevar a cabo la revisión.</li> <li>II. Cómo y con qué frecuencia se llevan a cabo las inspecciones de las cercas y/o bardas perimétricas.</li> <li>III. Cómo se lleva el registro de la inspección.</li> <li>IV. Quién es el responsable de verificar que las reparaciones y/o modificaciones cumplan con las especificaciones técnicas y requisitos de seguridad necesarias.</li> </ol>
<b>2.4 Estacionamientos.</b>	
<p>El acceso a los estacionamientos debe ser controlado y monitoreado por el personal de seguridad o designado para esta tarea se debe prohibir que los vehículos privados (de empleados, visitantes, proveedores y contratistas, entre otros) se estacionen fuera de los espacios asignados, que obstruyan las vialidades internas del parque, los accesos a los puntos de control e inspección y en su caso, a cualquier otro punto de acceso al mismo.</p>	

<b>Respuesta:</b>	<b>Notas Explicativas:</b>
	<p>Describir el procedimiento para el control y monitoreo de los estacionamientos, asegúrese de incluir los siguientes puntos:</p> <ol style="list-style-type: none"> <li>I. Responsables de controlar y autorizar el acceso a los estacionamientos de áreas comunes.</li> <li>II. Identificar señalización de los estacionamientos de uso común o compartido (especificar si los estacionamientos asignados a los propietarios e inquilinos del parque, se encuentran separados del patio de maniobras para vehículos de carga).</li> <li>III. Cómo se lleva a cabo el control de entrada y salida de vehículos a las instalaciones (indicar los registros que se realizan para el control del estacionamiento de uso común o compartido, los mecanismos de control existentes (por ejemplo: tarjetones, tarjetas lectoras, corbatines, etcétera), cómo se asignan y el área responsable de hacerlo.).</li> <li>IV. Identificar y señalar del estacionamiento de uso común o compartido.</li> </ol>
<b>2.5 Control de llaves y dispositivos de cerraduras.</b>	
<p>Las ventanas, puertas, casetas, plumas de acceso, rejas interiores y exteriores, de acuerdo a su análisis de riesgo, deben asegurarse con dispositivos de cierre. Todas las empresas del parque industrial sin excepción, deben contar con un procedimiento documentado para el manejo y control de llaves y/o dispositivos de cierre de las áreas interiores y exteriores que se hayan considerado como críticas. Asimismo, deben llevar un registro y establecer cartas responsivas firmadas por las personas que cuentan con llaves o accesos autorizados conforme a su nivel de responsabilidad y labores dentro de su área de trabajo.</p>	
<b>Respuesta:</b>	<b>Notas Explicativas:</b>
	<p>Indicará si todas las puertas, ventanas, casetas, plumas de acceso, ventanillas y rejas interiores y exteriores disponen de mecanismos de apertura y cierre manual o electrónico.</p> <p>Anexar el procedimiento documentado para el manejo y control de llaves y/o dispositivos de cierre, asegúrese que incluya los siguientes puntos:</p> <ol style="list-style-type: none"> <li>I. Responsables de administrar y controlar la seguridad de las llaves.</li> <li>II. Formato y/o registro de control para el préstamo de llaves.</li> <li>III. Tratamiento de pérdida o no devolución de llaves.</li> <li>IV. Señalar si existen áreas en las que se acceda con dispositivos electrónicos y/o algún otro mecanismo de acceso.</li> </ol>

<b>2.6 Alumbrado.</b>	
El alumbrado del perímetro interior y exterior del parque industrial debe permitir una clara identificación de personas, material y/o equipo que ahí se encuentre, incluyendo las siguientes áreas: entradas y salidas, bardas perimetrales, cercas interiores, carga, descarga y áreas de estacionamiento, debiendo contar con un sistema de emergencia y/o respaldo en las áreas sensibles de uso común.	
<b>Respuesta:</b>	<b>Notas Explicativas:</b>
	<p>Describir el procedimiento para la operación y mantenimiento del sistema de iluminación, asegúrese de incluir los siguientes puntos:</p> <ol style="list-style-type: none"> <li>I. Señalar qué áreas de uso común o compartidas se encuentran iluminadas y cuáles cuentan con sistema de respaldo (indique si cuenta con una planta de poder auxiliar o algún otro mecanismo para suministrar energía eléctrica en caso de alguna contingencia).</li> <li>II. De qué manera se cerciora que el sistema de iluminación sea el apropiado en cada una de las áreas donde se encuentran las empresas del parque industrial, de manera que permita una clara identificación del personal, material y/o equipo que ahí se encuentra.</li> <li>III. Responsable del control y mantenimiento de los sistemas de iluminación.</li> <li>IV. Programa de mantenimiento y revisión (en caso de coincidir con otro proceso, indicarlo).</li> <li>V. Protocolo de emergencia del centro de monitoreo del parque industrial en caso de apagón, catástrofes naturales o sabotaje.</li> </ol> <p>El procedimiento podrá incluir:</p> <ol style="list-style-type: none"> <li>I. Cómo se controla el sistema de iluminación.</li> <li>II. Horarios de funcionamiento.</li> <li>III. Identificación de áreas que requieren iluminación permanente.</li> </ol>

<b>2.7 Aparatos de comunicación.</b>	
Todas las empresas del parque industrial sin excepción, deben contar con aparatos y/o sistemas de comunicación para contactar de forma inmediata a su personal de seguridad, al centro de monitoreo del parque y a las autoridades en caso de ocurrir una situación de emergencia y seguridad. Adicionalmente, se debe de contar con un sistema de respaldo y verificar su buen funcionamiento de manera periódica.	
<b>Respuesta:</b>	<b>Notas Explicativas:</b>
	<p>Describir el procedimiento que el personal debe seguir para contactar al personal de seguridad del centro de monitoreo del parque industrial o, en su caso, a la autoridad correspondiente en caso de algún incidente de seguridad.</p> <p>Indicar si el personal operativo y administrativo de las empresas del parque cuentan o disponen con aparatos (teléfonos fijos, móviles, botones de alerta y/o emergencia, etcétera) para comunicarse con el personal de seguridad y/o con quien corresponda (estos deberán estar accesibles a los usuarios para poder tener una pronta reacción).</p> <p>Indicar qué tipo de aparatos de comunicación utiliza el personal de seguridad del parque industrial (teléfonos fijos, celulares, radios, sistema de alarma, etcétera).</p> <p>Describir el procedimiento para el control y mantenimiento de los aparatos de comunicación, asegúrese de incluir los siguientes puntos:</p> <ol style="list-style-type: none"> <li>I. Políticas de asignación de aparatos de comunicación móvil.</li> <li>II. Programa de mantenimiento o reemplazo de aparatos de comunicación fija y móvil.</li> <li>III. Indicar si cuenta con aparatos de comunicación de respaldo, cuando el sistema permanente fallara, y en su caso, describa brevemente.</li> </ol> <p>El procedimiento podrá incluir:</p> <ol style="list-style-type: none"> <li>I. Responsable del buen funcionamiento y mantenimiento de los aparatos de comunicación.</li> <li>II. Registros de verificación y mantenimiento de los aparatos.</li> <li>III. Forma de asignación de los aparatos de comunicación.</li> </ol>

## 2.8 Sistemas de alarma y de circuito cerrado de televisión y video vigilancia.

Los sistemas de alarma y de circuito cerrado de televisión y video vigilancia y las tecnologías de seguridad, se deben utilizar para vigilar, notificar o disuadir accesos no autorizados y actividades prohibidas en las instalaciones y demás áreas consideradas sensibles, notificar al área correspondiente, además de utilizarse como herramienta de prueba en investigaciones derivadas de algún incidente de seguridad.

El Parque Industrial debe contar con un centro de monitoreo propio o de administración tercerizada, así mismo, estos sistemas y tecnologías de seguridad, deberán colocarse de acuerdo a un análisis de riesgo previo, de tal forma que se mantengan vigiladas y monitoreadas las áreas de acceso de personal, visitantes, proveedores, vehículos de pasajeros, carga y además áreas consideradas sensibles. Dichos sistemas de alarma y de circuito cerrado de televisión y video vigilancia deben permitir una clara identificación del área o ambiente que vigila, estar permanentemente grabando y mantener un respaldo de las grabaciones por lo menos de un mes, con la finalidad de tener los elementos necesarios para deslindar las responsabilidades correspondientes en caso de un incidente de seguridad.

Los sistemas de alarma y de circuito cerrado de televisión y video vigilancia y las tecnologías de seguridad, deben contar con un procedimiento documentado de operación que incluya la supervisión del buen estado del equipo y la verificación de la correcta posición de las cámaras, indicando la frecuencia con la que debe realizar el respaldo de las grabaciones, así como los responsables de su operación. Dicho sistema y toda la infraestructura de tecnología de seguridad deberá tener un acceso restringido.

### Respuesta:

### Notas Explicativas:

Mencionar el procedimiento documentado en el que indique el funcionamiento del sistema central de alarmas externo o sensores, y en su caso, describa los siguientes puntos:

- I. Indicar si todas las puertas y ventanas tienen sensores de alarma, así como las áreas donde se cuenta con sensores de movimiento.
- II. Procedimiento a seguir en caso de activarse una alarma.
- III. Indicar el personal o área responsable de dar mantenimiento, cómo se reportan fallas y los registros que utilizan.

Describir el procedimiento documentado para la operación de los sistemas de alarma y de circuito cerrado de televisión y video vigilancia y las tecnologías de seguridad (este debe revisarse y actualizarse anualmente y de acuerdo con el análisis de riesgo o las circunstancias), asegúrese de incluir los siguientes puntos:

- I. Indicar el número de cámaras de seguridad de los sistemas de alarma y de circuito cerrado de televisión y video vigilancia instaladas, y su ubicación por áreas (detalle si cubre los puntos de entrada y salida de las instalaciones, para cubrir el movimiento de vehículos e individuos). Anexe un layout o mapa de distribución de las cámaras de seguridad.

	<ul style="list-style-type: none"><li><b>II.</b> Señalar la ubicación de los sistemas de alarma y de circuito cerrado de televisión y video vigilancia y las tecnologías de seguridad, dónde se localizan los monitores, quién los revisa, así como los horarios de operación, y en su caso, si existen estaciones de monitoreo remoto. Toda la infraestructura de tecnología de seguridad debe estar protegida físicamente contra el acceso no autorizado.</li><li><b>III.</b> Se deben realizar revisiones periódicas y aleatorias de las grabaciones. Indique de qué forma las revisan (aleatoria, cada semana, eventos especiales, áreas restringidas, etcétera), quién es el personal designado y cómo la gerencia se involucra en las revisiones. Los resultados de las revisiones deben documentarse para incluir acciones correctivas para fines de auditoría.</li><li><b>IV.</b> Indicar por cuánto tiempo se mantienen estas grabaciones (debiendo ser por lo menos de un mes).</li><li><b>V.</b> Los sistemas de alarma y de circuito cerrado de televisión y video vigilancia y las tecnologías de seguridad deben de contar con una fuente de energía alternativa que permita que estos continúen funcionando en caso de una pérdida inesperada de energía directa. Por lo anterior, indique si los sistemas de alarma y de circuito cerrado de televisión y video vigilancia se encuentran respaldados por una planta de poder eléctrica o algún otro mecanismo para suministrar energía eléctrica, que garantice su funcionamiento. Estos sistemas deberían de tener una función de alarma/notificación, que indique una condición de falla en el funcionamiento y/ o grabación, señale si sus sistemas tienen dicha función.</li><li><b>VI.</b> Indicar si adicionalmente a los sistemas de alarma y de circuito cerrado de televisión y video vigilancia, utiliza algún otro tipo de tecnología para robustecer las medidas de seguridad con las que ya cuenta.</li></ul>
--	--

	<p><b>VII.</b> Describir el procedimiento que se ha implementado para probar e inspeccionar de manera regular los sistemas de alarma y de circuito cerrado de televisión y video vigilancia y las tecnologías de seguridad y asegurar su buen funcionamiento. Los resultados de las inspecciones y las pruebas de funcionamiento deben estar documentadas, al igual que las acciones correctivas necesarias (estas se deben implementar lo antes posible). Adicionalmente, que los resultados documentados de estas inspecciones se mantengan durante un tiempo suficiente para fines de auditoría.</p> <p><b>VIII.</b> Indicar si el proveedor de sistemas de alarma y de circuito cerrado de televisión y video vigilancia, tiene acceso a las cámaras de seguridad, si es el encargado de realizar el monitoreo de las mismas, de forma se controlan los accesos y quién es el responsable de dicho monitoreo.</p>
<p><b>3. Controles de acceso físico.</b></p>	
<p>Los controles de acceso físico, son mecanismos o procedimientos que previenen e impiden la entrada no autorizada a las instalaciones, mantienen control del ingreso de los empleados, proveedores y visitantes, protegiendo los activos del parque industrial y de las empresas domiciliadas en él.</p> <p>Los controles de acceso deben incluir la identificación y control de todos los empleados, visitantes y proveedores en todos los puntos de entrada. Así mismo, se deben mantener registros y evaluar permanentemente los mecanismos o procedimientos documentados de ingreso a las instalaciones, siendo la base para comenzar a integrar la seguridad como una de las funciones primordiales dentro de cualquier parque industrial.</p>	
<p><b>3.1 Personal de Seguridad.</b></p>	
<p>El parque industrial debe contar con personal de seguridad y vigilancia. Este personal desempeña un rol importante en la protección física de las instalaciones y de la seguridad de los activos del parque industrial y de las empresas instaladas en él, así como para controlar el acceso y salida de todas las personas y vehículos al inmueble.</p> <p>El personal de seguridad, debe contar con un procedimiento documentado para llevar a cabo sus funciones y tener pleno conocimiento de los mecanismos y procedimientos en situaciones de emergencia, detección y retiro de personas no autorizadas o cualquier incidente de seguridad ocurrido dentro del parque industrial. La gerencia debe verificar periódicamente el cumplimiento de los procedimientos políticas y funciones a través de auditorías internas con el objetivo de verificar su correcta ejecución.</p>	
<p><b>Respuesta:</b></p>	<p><b>Notas Explicativas:</b></p>
	<p>Anexar el procedimiento documentado para la operación del personal de seguridad (roles o consignas) y asegúrese de incluir los siguientes puntos:</p> <ol style="list-style-type: none"> <li><b>I.</b> Indicar el número de personal de seguridad que custodia el parque industrial.</li> <li><b>II.</b> Señalar los cargos y/o funciones del personal y horarios de operación.</li> </ol>

	<p><b>III.</b> En caso de contratarse un servicio externo, proporcionar los datos generales de la empresa (clave en el RFC, razón social, domicilio), y especificar número del personal empleado, detalles de operaciones, registros y reportes que utilizan para desempeñar sus funciones.</p> <p><b>IV.</b> En caso de contar con personal armado, describa el procedimiento para el control y resguardo de las armas, presentar evidencia de los registros y permisos expedidos por las autoridades competentes en la materia.</p>
<p><b>3.2 Identificación de los empleados.</b></p>	
<p>Debe existir un sistema de identificación de empleados con fines de acceso a las instalaciones del parque industrial. Los empleados sólo deben tener acceso a aquellas áreas que necesiten para desempeñar sus funciones. La gerencia o el personal de seguridad del parque industrial, y de las compañías instaladas en el deben controlar adecuadamente la entrega y devolución de insignias, gafetes y/o credenciales de identificación de empleados, visitantes y proveedores. Se deben documentar los procedimientos para la entrega, devolución y cambio de dispositivos de acceso (por ejemplo: llaves, gafetes y/o credenciales, tarjetas de proximidad, etcétera). El acceso a las áreas sensibles debe estar restringido según la descripción del trabajo o las tareas asignadas.</p>	
<p><b>Respuesta:</b></p>	<p><b>Notas Explicativas:</b></p>
	<p>Describir el procedimiento para la identificación de los empleados y asegúrese de incluir los siguientes puntos:</p> <p><b>I.</b> Mecanismos de identificación (credencial y/o gafete con foto, control de acceso, biométricos, tarjetas de proximidad, etcétera).</p> <p><b>II.</b> Indicar si los empleados utilizan uniformes, cómo son asignados (por puestos, área, funciones, etcétera) y retirados (en su caso).</p> <p><b>III.</b> Indicar cómo se identifica al personal contratado por un socio comercial que labore dentro de las instalaciones (seguridad, limpieza, mantenimiento, contratistas, etcétera).</p> <p>El procedimiento también debe de describir cómo el parque industrial entrega, cambia y retira las identificaciones y controles de acceso del empleado y asegúrese de incluir las áreas responsables de autorizarlas y administrarlas.</p> <p>Indicar cómo asegura que el acceso a las áreas sensibles este restringido según la descripción del trabajo o las tareas asignadas (incluya el tipo de registros y controles que utiliza).</p> <p>Anexar el procedimiento documentado para el control de las identificaciones.</p>

### 3.3 Identificación de visitantes y proveedores.

Para tener acceso a las instalaciones los visitantes, proveedores y contratistas deben presentar identificación oficial con fotografía con fines de documentación a su llegada y se deberá llevar un registro. Todos los visitantes, proveedores y contratistas deben recibir una identificación temporal, estar acompañados por personal de la empresa durante su permanencia en las instalaciones y asegurarse que el visitante/proveedor/contratista porte siempre en un lugar visible la identificación provisional proporcionada. Este procedimiento deberá estar documentado.

Respecto a los vehículos de carga que ingresan al parque industrial, deberá de contar con un control que permita verificar el medio de transporte, contenedor, carros de tren, remolques y/o semirremolques, con la finalidad de identificar y mitigar el riesgo de contaminación del parque con productos ilícitos.

Respuesta:	Notas Explicativas:
	<p>Anexar el procedimiento para el control de acceso de los visitantes, proveedores y contratistas, asegúrese de incluir los siguientes puntos:</p> <ul style="list-style-type: none"><li>I. Señalar qué registros se llevan a cabo (formatos personales por cada visita, bitácoras, entre otros).</li><li>II. El registro de visitantes y proveedores debe incluir lo siguiente:<ul style="list-style-type: none"><li>a) Fecha de la visita.</li><li>b) Nombre del visitante.</li><li>c) Número de identificación con foto (documentos oficiales como: licencia de manejo, pasaporte, INE, etcétera).</li><li>d) Hora de entrada y de salida.</li><li>e) En el caso de acceso vehicular el formato deberá incluir los datos del vehículo particular o de carga (modelo, placa, número de remolque, etcétera).</li></ul></li><li>III. Señalar quién es la persona responsable de acompañar al visitante y/o proveedor y si existen áreas restringidas para su ingreso.</li><li>IV. Describir el tipo de control o medidas de seguridad que tiene implementadas respecto al ingreso de los vehículos de carga (medios de transporte, contenedores, carros de tren, remolques y/o semirremolques, etcétera), con la finalidad de identificar y mitigar el riesgo de contaminación del parque con productos ilícitos.</li></ul>

<b>3.4 Procedimiento de identificación y retiro de personas o vehículos no autorizados.</b>	
El centro de monitoreo del Parque Industrial debe contar con un procedimiento documentado que especifique cómo identificar, enfrentar o reportar a personas y/o vehículos no autorizados o identificados, dicho procedimiento debe ser comunicado al personal responsable mediante capacitación. La capacitación debe estar documentada.	
<b>Respuesta:</b>	<b>Notas Explicativas:</b>
	<p>Anexar el procedimiento documentado para identificar, enfrentar o reportar personas y/o vehículo no autorizados o identificados.</p> <p>El procedimiento deberá incluir:</p> <ol style="list-style-type: none"> <li>I. Personal responsable.</li> <li>II. Designar a una persona o área responsable para ser informado de los incidentes de seguridad.</li> <li>III. Indicaciones para enfrentar y dirigirse al personal no identificado.</li> <li>IV. Señalar en qué casos deberá reportarse a las autoridades correspondientes.</li> <li>V. Cómo se lleva a cabo el registro de los incidentes de seguridad y las medidas adoptadas para cada caso.</li> </ol>
<b>3.5 Entregas de mensajería y paquetería.</b>	
El personal del centro de monitoreo debe identificar al personal de las empresas de mensajería y paquetería y autorizar su ingreso para distribuir y entregar la correspondencia dirigida a las empresas ubicadas al interior del parque industrial.	
<b>Respuesta:</b>	<b>Notas Explicativas:</b>
	<p>Anexar el procedimiento para identificar y autorizar el ingreso del personal de las empresas de mensajería que distribuye y entrega la correspondencia destinada a las empresas instaladas en el parque industrial y asegúrese de incluir lo siguiente:</p> <ol style="list-style-type: none"> <li>I. Cómo identifica al personal o proveedor del servicio de mensajería y paquetería (señale si requiere de procedimiento adicional al de acceso a proveedores).</li> </ol>
<b>4. Socios comerciales.</b>	
<p>El Corporativo del parque industrial debe contar con procedimientos escritos y verificables para la selección de propietarios e inquilinos, así como para la selección y contratación de nuevos socios comerciales y monitoreo de los socios con los que ya se encuentra trabajando, como: proveedores de servicios de limpieza, seguridad privada, contratación de personal, jardinería, contratistas, colocación y mantenimiento de los sistemas de alarma y de circuito cerrado de televisión y video vigilancia, proveedores de sistemas y Tecnologías de la Información, entre otros, y de acuerdo a su análisis de riesgo, exigir que cumplan con las medidas de seguridad para fortalecer la cadena de suministros internacional.</p> <p>El análisis de riesgo que realice el Corporativo del parque industrial respecto a sus socios comerciales (clientes y proveedores), deberá incluir riesgos relacionados con la identificación de actividades relacionadas con el lavado de dinero y la financiación del terrorismo. Adicionalmente, el parque industrial debe fomentar una política y un programa de cumplimiento social documentado que, como mínimo, aborde cómo entre sus empleados y socios comerciales podrían garantizar que los bienes, insumos o mercancías nacionales e importadas a México para la elaboración de productos o mercancías, no provienen de la extracción, producción o fabricación total o parcialmente, con formas prohibidas de trabajo, es decir, forzoso u obligado, incluido el trabajo infantil forzoso u obligado, al amparo del artículo 23.6 del T-MEC y el Acuerdo que establece las mercancías cuya importación está sujeta a regulación a cargo de la Secretaría del Trabajo y Previsión Social, publicado en el DOF el 17 de febrero de 2023.</p>	

<b>4.1 Criterios de selección.</b>	
<p>Deben existir procedimientos documentados para la selección, seguimiento y renovación de relaciones comerciales con los asociados de negocio o proveedores, que incluyan entrevistas, verificación de referencias, métodos de evaluación y uso de la información proporcionada. La información derivada de la investigación y/o evaluación de los asociados de negocio y/o proveedores deberá documentarse y estar integrada en un expediente (físico o electrónico). El procedimiento para la selección de socios comerciales deberá incluir, indicadores para identificar clientes o proveedores que podrían no ser legítimos o con domicilios no localizados, además de investigaciones, revisiones o evaluaciones de dichos socios para la identificación y control de las actividades relacionadas con el lavado de dinero y la financiación del terrorismo. Si la investigación y/o evaluación de algún socio comercial conduce a dudas sustanciales sobre la veracidad de sus operaciones o servicios, la empresa deberá evitar su contratación y, en su caso, notificar a su especialista de seguridad o contacto del Programa Operador Económico Autorizado y a la autoridad correspondiente sobre sus sospechas.</p>	
<b>Respuesta:</b>	<b>Notas Explicativas:</b>
	<p>Anexar el procedimiento documentado para la selección y contratación de nuevos socios comerciales y monitoreo de los socios con los que ya se encuentra trabajando, esto comprende cualquier cliente o proveedor de bienes o servicios que tenga una relación comercial con el parque industrial (es en el siguiente sub-estándar donde se solicita diferenciar aquellos de riesgo en su cadena de suministros), asegúrese de incluir los siguientes puntos:</p> <ol style="list-style-type: none"> <li>I. Qué información es requerida al socio comercial.</li> <li>II. Qué aspectos son revisados e investigados en la selección y contratación de proveedores, así como para la venta de un predio, o el alquiler de una nave industrial, almacén, etcétera.</li> <li>III. Los indicadores para identificar clientes o proveedores que podrían no ser legítimos (pagos por encima de la tarifa estándar, en efectivo; tener poco conocimiento de la mercancía que se va a enviar; ser evasivo; información de contacto mínima (teléfono celular, puntos de contacto, correos electrónicos, entre otros); empresas de reciente creación o negocios sin historial comercial, etcétera) o con domicilios no localizados. Este punto refiere a señalar todas aquellas alertas para determinar que un socio comercial no es confiable y así, realizar una investigación más profunda y evaluar si se debe trabajar con él.</li> <li>IV. Indicar si mantiene un expediente de cada uno de sus socios comerciales (copropietarios, arrendatarios y proveedores).</li> </ol>

	<p><b>V.</b> Señalar de qué manera se evalúan los servicios de sus proveedores y qué puntos se revisan.</p> <p><b>VI.</b> Listado actualizado con los datos generales de las empresas que operan en el parque industrial al momento de presentar la solicitud de inscripción (nombre, clave en el RFC, giro o actividad preponderante, indique si realizan o no operaciones de comercio exterior, etcétera), en caso de alta o baja de copropietarios o arrendatarios deberá dar aviso a la autoridad.</p> <p>El expediente debe incluir como mínimo lo siguiente:</p> <p><b>I.</b> Datos de la empresa que alberga (nombre, clave en el RFC, giro o actividad preponderante, etcétera).</p> <p><b>II.</b> Copia simple del acta constitutiva.</p> <p><b>III.</b> Identificación y copia simple del poder notarial del representante legal.</p> <p><b>IV.</b> Comprobante de domicilio.</p> <p><b>V.</b> Referencias comerciales (en su caso).</p> <p><b>VI.</b> Contratos, acuerdo y/o convenios de confidencialidad.</p> <p><b>VII.</b> Políticas de seguridad.</p> <p><b>VIII.</b> En su caso, certificado o número de certificación en los programas de seguridad a lo que pertenezcan.</p>
<p><b>4.2 Requerimientos en seguridad.</b></p>	
<p>El parque industrial debe contar con un procedimiento documentado en el que de acuerdo con su análisis de riesgos, solicite requisitos adicionales en materia de seguridad a aquellos socios comerciales (empresas copropietarias o arrendatarias) que realicen operaciones de comercio exterior.</p> <p>En el caso de los socios comerciales que intervengan en su cadena de suministros, ya sea como proveedores que presten sus servicios en el interior del parque industrial como: empresas de seguridad privada, limpieza, mantenimiento, contratación de personal, jardinería, contratistas, colocación y mantenimiento de los sistemas de alarma y de circuito cerrado de televisión y video vigilancia, proveedores de sistemas y Tecnologías de la Información, entre otros, están obligados al cumplimiento de los mismos requisitos de seguridad en la cadena de suministro.</p> <p>Los requisitos deberán estar basados en el "Perfil de Parques Industriales" establecido por la AGACE, o en caso de existir, el Perfil específico para cada actor de la cadena de suministros que le corresponda.</p> <p>El parque industrial debe solicitar a sus socios comerciales la documentación que acredite y compruebe que cumple con los estándares mínimos de seguridad establecidos en este "Perfil de Parques Industriales", ya sea a través de una declaración escrita emitida por el representante legal del socio, convenios o cláusulas contractuales, respaldado con documentación que avale el cumplimiento de los requisitos establecidos en el Programa Operador Económico Autorizado. De igual manera, la empresa debe tener en cuenta y conocer los requisitos específicos del Programa Operador Económico Autorizado que serán aplicables a cada uno de sus socios comerciales, en función de su actividad dentro de la cadena de suministro.</p> <p>Todas las empresas copropietarias o arrendatarias deben adherirse -sin excepción- a la política y al protocolo general de seguridad establecida por el parque industrial.</p>	

Respuesta:	Notas Explicativas:
	<p>Describir el procedimiento que indique cómo lleva a cabo la identificación de socios comerciales que requieren cumplir con estándares mínimos en materia de seguridad. Asegúrese de incluir los siguientes puntos:</p> <ol style="list-style-type: none"> <li>I. Un registro de los socios comerciales (empresas copropietarias o arrendatarias y proveedores) que realizan operaciones de comercio exterior, que intervengan en su cadena de suministro y deben cumplir con los requisitos en materia de seguridad. Mencione qué tipo de empresas son estas.</li> <li>II. Indicar de qué forma documental (convenios, cláusulas contractuales y/o adendas) asegura que sus socios comerciales (empresas copropietarias o arrendatarias y proveedores) cumplen con los requisitos en materia de seguridad.</li> <li>III. Indicar si existen convenios, acuerdos, cláusulas contractuales y/o adendas respecto a la implementación de medidas de seguridad con proveedores de servicios al interior del parque industrial, tales como: seguridad privada, servicio de limpieza y mantenimiento, comedor, jardinería, proveedor de Tecnologías de la Información, etcétera.</li> <li>IV. Indicar si cuenta con socios comerciales que se les exija pertenezcan a un programa de seguridad de la cadena de suministros (por ejemplo: CTPAT o algún Programa Operador Económico Autorizado de la OMA), así como la información y documentación que le son solicitadas.</li> </ol>
<b>4.3 Revisiones del socio comercial.</b>	
<p>El parque industrial, a través del Comité de Seguridad debe realizar evaluaciones periódicas de seguridad (así como derivadas de situaciones de riesgo), de los procesos e instalaciones de los asociados de negocio con base a un análisis de riesgo, para garantizar que cuentan con estándares mínimos en materia de seguridad requeridos por el parque industrial, basados en el Programa Operador Económico Autorizado, mantener registros de las mismas que permitan constatar que los procesos y medidas de seguridad se están ejecutando, así como del seguimiento correspondiente.</p> <p>Cuando se encuentren inconsistencias, el parque industrial deberá comunicarlo a su socio y proveedor y proporcionar un período razonable para atender las observaciones o áreas de oportunidad identificadas o, en caso contrario, tener las medidas necesarias para sancionarla.</p> <p>Realizar evaluaciones de seguridad de los socios comerciales es importante para garantizar que exista un programa de seguridad sólido y que funcione correctamente, es por eso que, además de un procedimiento documentado debe existir un programa o calendario para la ejecución de dichas revisiones o evaluaciones de seguridad priorizando a los socios que son más críticos conforme a su análisis de riesgo. Si un miembro no es evaluado y la empresa desconoce si los procesos e instalaciones de sus socios comerciales funcionan correctamente, ponen en riesgo su cadena de suministro.</p>	

Respuesta:	Notas Explicativas:
	<p>El parque industrial debe contar con un procedimiento documentado para realizar evaluaciones para la verificación o revisión de los requisitos en materia de seguridad en los procesos e instalaciones de socios comerciales. Describa el procedimiento para realizar las revisiones de sus socios comerciales, asegúrese de incluir los siguientes puntos:</p> <ol style="list-style-type: none"> <li>I. Periodicidad con la que realiza las visitas al socio comercial (esta debe de ser por lo menos una vez al año y derivadas de situaciones de riesgo).</li> <li>II. Programa o calendario para la ejecución de las revisiones de seguridad.</li> <li>III. Registro o reporte de la verificación o revisión y, en su caso, del seguimiento correspondiente.</li> <li>IV. El o los formatos de verificación tendrán que estar debidamente requisitados, colocando la fecha, nombre y cargo de quienes participan en la revisión, firmas, etcétera.</li> <li>V. Señalar qué medidas de acción se toman cuando los socios comerciales no cumplan con los requisitos de seguridad establecidos.</li> </ol> <p>En caso de tener socios comerciales que cuenten con la certificación CTPAT u otro programa de certificación de seguridad en la cadena de suministros, indique la periodicidad con la que es revisado su estatus, cómo lo registran y las acciones que toma en caso de detectarse que esté suspendido y/o cancelado, conforme a lo establecido en su procedimiento.</p> <p>El procedimiento deberá incluir:</p> <ol style="list-style-type: none"> <li>I. Periodicidad de las visitas.</li> <li>II. Puntos de revisión en materia de seguridad.</li> <li>III. Elaboración de reportes.</li> <li>IV. Retroalimentación y acuerdos con el socio comercial.</li> <li>V. Seguimiento a los acuerdos.</li> <li>VI. Medidas en caso de incumplimiento de los requisitos.</li> <li>VII. Registro de evaluaciones.</li> <li>VIII. Áreas o responsables de llevar a cabo este procedimiento.</li> </ol>

<b>5. Seguridad de procesos.</b>	
<p>Deben establecerse medidas de control para garantizar la efectividad de los procesos relacionados con la seguridad de los medios de transporte (en cualquiera de sus modalidades), manejo y almacenaje de mercancía de comercio exterior a lo largo de la cadena de suministro. Asimismo, deben existir procedimientos para impedir, detectar o disuadir que materiales no declarados, personal o vehículos no autorizados tengan acceso al parque industrial. Estas medidas de control y procedimientos deben documentarse con el objetivo de mantener en todo momento la integridad del medio de transporte y la mercancía desde el ingreso al parque industrial y hasta las instalaciones de las empresas copropietarias o arrendatarias.</p>	
<b>5.1 Entrega y recepción de carga.</b>	
<p>El parque industrial debe dar a conocer a los operadores/choferes de las compañías transportistas que entreguen o reciban mercancía de comercio exterior, las políticas y los lineamientos de seguridad al ingresar, circular y efectuar maniobras de carga/descarga al interior del parque.</p> <p>Por su parte, todas las empresas -sin excepción- deben informar previamente al personal de seguridad del parque industrial, los nombres de las compañías transportistas, el tipo de vehículos de carga y características de los sellos o candados normalmente utilizados y en su caso, los datos de operadores para que puedan ser plenamente identificados desde el ingreso al parque industrial y hasta las instalaciones de las empresas copropietarias o arrendatarias. El parque industrial debe contar con una base de datos actualizada que contenga toda la información anterior.</p>	
<b>Respuesta:</b>	<b>Notas Explicativas:</b>
	<p>El personal de seguridad debe actualizar permanentemente los datos de compañías transportistas, operadores, tipos de vehículos de carga que cotidianamente ingresan y egresan del Parque Industrial, así como las características distintivas de los sellos o candados de alta seguridad utilizados por las empresas ubicadas en su interior.</p>
<b>6. Seguridad de los vehículos de carga, contenedores, remolques y/o semirremolques.</b>	
<p>Se debe mantener la integridad en los medios de transporte, contenedores, carros de tren, remolques y semirremolques, para protegerlos contra la introducción de personas y/o materiales no autorizados. Por lo anterior, es necesario que las empresas ubicadas en el Parque Industrial tengan procedimientos documentados para revisar, sellar y mantener la integridad de los mismos.</p>	
<b>6.1 Almacenaje de vehículos, medios de transporte, contenedores, carros de tren, remolques y semirremolques.</b>	
<p>Cuando los tractos, camiones rabones, furgonetas, van, cajas secas, cajas refrigeradas, furgones, góndolas, carros-tanque, tolvas de ferrocarril, etcétera, que transporten mercancías de comercio exterior estén vacíos y deban pernoctar y resguardarse en el interior del parque industrial, deben asegurarse con un sello indicativo, o bien, colocarse en un área común vigilada y monitoreada para impedir el acceso y manipulación indebida. Los medios de transporte no deben obstruir las vialidades internas del Parque Industrial. Si por causa de fuerza mayor, los contenedores, remolques o semi remolques deben permanecer más de un día en el Parque, deben permanecer al interior de la empresa que solicitó el servicio, o bien, si la extensión e infraestructura del Parque lo permiten, en un área común que cumpla con las medidas de seguridad antes mencionadas.</p> <p>Cuando por necesidades de la operación se tenga que resguardar algún contenedor, remolque o semirremolque cargado con mercancía de comercio exterior, este debe posicionarse en un área segura y monitoreada por los sistemas de alarma y de circuito cerrado de televisión y video vigilancia, para impedir el acceso no autorizado y la manipulación de la mercancía, por lo que debe estar cerrado con un candado de alta seguridad de acuerdo a la Norma ISO 17712. Cuando la carga sea almacenada durante la noche o durante un período prolongado, deben tomarse medidas para asegurar la carga contra el acceso no autorizado.</p>	

Respuesta:	Notas Explicativas:
	Indicar si al interior del Parque Industrial se almacenan contenedores, remolques y/o semirremolques llenos o vacíos para su despacho posterior, y explique de qué manera se mantiene la integridad de los mismos dentro de sus instalaciones.
<b>7. Seguridad del personal.</b>	
Se debe contar con procedimientos documentados para el registro y evaluación de personas que desean obtener un empleo en el Corporativo del Parque Industrial y establecer métodos para realizar verificaciones periódicas de los empleados actuales.	
También, deben existir programas de capacitación continuos para el personal administrativo y de seguridad que difundan las políticas de seguridad que rigen al interior del Parque Industrial, así como las consecuencias y acciones a tomar en caso de cualquier falta.	
<b>7.1 Verificación de antecedentes laborales.</b>	
El Parque Industrial debe tener procedimientos documentados para investigar y verificar la información asentada en el currículo, antecedentes criminales (si la legislación y políticas de la empresa lo permiten) y solicitud de los candidatos con posibilidad de empleo, de conformidad con la legislación local, ya sea por cuenta propia o por medio de una empresa externa.	
De igual forma, para los cargos que por su sensibilidad así lo requieran y afecten la seguridad del Parque Industrial, de conformidad con el análisis de riesgo efectuado previamente, deben considerar solicitar requisitos más estrictos para su contratación, los cuales se deben actualizar de manera periódica. Respecto al personal que ya labora en la compañía, se deben realizar investigaciones periódicas en función de las funciones y/o la sensibilidad del puesto del empleado.	
Toda la información referente al personal deberá mantenerse en expedientes personales, mismos que deben tener un acceso restringido.	
Respuesta:	Notas Explicativas:
	<p>Describir el procedimiento documentado para la contratación del personal, y asegúrese de incluir lo siguiente:</p> <ol style="list-style-type: none"> <li>I. Requisitos y documentación exigida.</li> <li>II. Pruebas y exámenes solicitados.</li> </ol> <p>Indicar las áreas y/o puestos críticos que se hayan identificado como de riesgo, conforme a su análisis y señale lo siguiente:</p> <ol style="list-style-type: none"> <li>I. Indicar si existen requisitos adicionales para áreas y/o puestos de trabajo específicos. Como antecedentes criminales (si la legislación y las políticas de la empresa lo permiten), carta de antecedentes no penales, estudios socioeconómicos, estudios clínicos toxicológicos (uso de drogas) etcétera. En su caso, señale los puestos o áreas de trabajo en que se requieren y con qué periodicidad se llevan a cabo.</li> <li>II. Indicar si previo a la contratación, el candidato debe firmar un acuerdo de confidencialidad o un documento similar.</li> </ol>

	<p>En caso de utilizar los servicios de una agencia para la contratación de personal, indique si esta cuenta con un procedimiento documentado para la contratación de personal y cómo se asegura de que lo cumplan.</p> <p>Los procedimientos para la contratación del personal y contratistas podrán incluir:</p> <ol style="list-style-type: none"> <li>I. Investigaciones exhaustivas de los antecedentes laborales y personales de los nuevos empleados.</li> <li>II. Cláusulas de confidencialidad y responsabilidad en los contratos de los empleados.</li> <li>III. Requisitos específicos para puestos críticos.</li> <li>IV. En su caso, la actualización periódica del estudio socioeconómico o de laboratorio clínico de los empleados que trabajen en áreas críticas y/o sensibles.</li> <li>V. Proceso de contratación y requisitos que solicitan para los empleados temporales y contratistas.</li> </ol>
<p><b>7.2 Procedimiento para baja del personal.</b></p>	
<p>Deben existir procedimientos documentados para la baja del personal en los que se incluya la entrega de identificaciones y cualquier otro artículo que se le haya proporcionado para realizar sus funciones (llaves, uniformes, gafetes y/o credenciales, equipo informático, contraseñas, aparatos de comunicación, herramientas, etcétera). Asimismo, este procedimiento debe incluir la baja en aquellos sistemas informáticos, de accesos, entre otros que pudieran existir.</p>	
<p><b>Respuesta:</b></p>	<p><b>Notas Explicativas:</b></p>
	<p>Describir el procedimiento para la baja del personal, y asegúrese de incluir lo siguiente:</p> <ol style="list-style-type: none"> <li>I. Quién es el responsable de llevar a cabo y dar seguimiento a este procedimiento.</li> <li>II. Cómo se realiza y confirma la entrega de identificaciones, uniformes, llaves y demás equipo.</li> <li>III. Indicar el control, registro y/o formato, en el que se identifique y asegure la entrega de material y baja en sistemas informáticos (en su caso, anexas).</li> <li>IV. Señalar el tipo de registros del personal que finalizó su relación laboral con el Parque Industrial, para que cuando haya sido por motivos de seguridad, se prevenga a las empresas inquilinas, proveedores de servicios y/o asociados de negocio.</li> </ol>

<b>7.3 Administración de personal.</b>	
<p>El Corporativo del Parque Industrial debe mantener un sistema, control o base de datos de empleados activos actualizada. Asimismo, debe realizar y mantener actualizados los registros de afiliación a instituciones de seguridad social y demás registros legales de orden laboral.</p> <p>En el caso de que el Parque Industrial cuente con personal contratado por sus socios comerciales y labore dentro de sus instalaciones, debe asegurarse de que cumplan con los mismos requisitos que el resto de sus empleados.</p>	
<b>Respuesta:</b>	<b>Notas Explicativas:</b>
	<p>Indicar si el parque industrial cuenta con un sistema, control o base de datos actualizada, tanto del personal contratado directamente, como aquel contratado a través de una empresa proveedora de servicios y asegúrese que incluya de forma enunciativa mas no limitativa los siguientes puntos:</p> <ol style="list-style-type: none"> <li><b>I.</b> Nombre completo.</li> <li><b>II.</b> Fotografía actualizada mínimo cada cinco años.</li> <li><b>III.</b> Datos personales (edad, nombre, fecha de nacimiento, número telefónico, domicilio, CURP, número de seguridad social, tipo sanguíneo, alergias, etcétera).</li> <li><b>IV.</b> Filiación.</li> <li><b>V.</b> Antecedentes laborales.</li> <li><b>VI.</b> Enfermedades.</li> <li><b>VII.</b> Exámenes médicos.</li> <li><b>VIII.</b> Capacitación.</li> <li><b>IX.</b> Exámenes Psicométricos.</li> <li><b>X.</b> Exámenes Toxicológicos.</li> <li><b>XI.</b> Resultados de evaluaciones periódicas.</li> <li><b>XII.</b> Observaciones.</li> </ol> <p>Este personal, deberá estar contratado de acuerdo con las leyes y reglamentos de orden laboral vigentes.</p>
<b>8. Seguridad de la información y documentación.</b>	
<p>Deben existir medidas de prevención para mantener la confidencialidad e integridad de la información y documentación generada por los sistemas, incluyendo aquellos utilizados para el intercambio de información con otros integrantes de la cadena de suministros. Asimismo, deben existir políticas y/o procedimientos integrales documentados para proteger los sistemas de Tecnologías de la Información, que incluyan las medidas contra su mal uso, además de identificar y priorizar acciones para reducir el riesgo de la ciberseguridad. También, podrían abordar cómo un miembro comparte información sobre amenazas de seguridad cibernética con el gobierno y otros socios comerciales.</p>	

<b>8.1 Clasificación y manejo de documentos.</b>	
<p>Deben existir procedimientos para clasificar documentos de acuerdo a su sensibilidad y/o importancia. La documentación sensible e importante debe ser almacenada en un área segura que solamente permita el acceso a personal autorizado. Se debe identificar el tiempo de vida útil de la documentación y establecer procedimientos para su destrucción.</p> <p>El Parque Industrial debe contar con expedientes resguardados y actualizados de las empresas copropietarias y arrendatarias con las que tiene relación de negocios, así como toda la información relativa a la seguridad de su cadena de suministro.</p> <p>El Parque Industrial debe conducir revisiones de forma regular para verificar los accesos a la información y asegurarse de que no sean utilizados de manera indebida.</p>	
<b>Respuesta:</b>	<b>Notas Explicativas:</b>
	<p>Anexar el procedimiento documentado para el registro, control y almacenamiento de documentación impresa (clasificación y archivo de documentos), debiendo incluir:</p> <ol style="list-style-type: none"> <li>I. Registro de control para entrega, préstamo, entre otros de documentación.</li> <li>II. Acceso restringido al área de archivos.</li> <li>III. Políticas de almacenamiento y clasificación.</li> <li>IV. Un plan de seguridad actualizado que describa las medidas en vigor relativas a la protección de los documentos contra accesos no autorizados, así como contra la destrucción deliberada o la pérdida de los mismos.</li> <li>V. Para el caso de información electrónica o digital, deberá apegarse a los criterios de seguridad del subestándar 8.2. Seguridad de la tecnología de la información.</li> </ol>
<b>8.2 Seguridad de la tecnología de la información.</b>	
<p>Para proteger los sistemas de Tecnologías de la Información contra amenazas comunes de ciberseguridad, una empresa debe contar con suficiente protección que impulse la seguridad en la infraestructura de Tecnologías de la información (software y hardware) contra malware (virus, spyware, gusanos, troyanos, etcétera), baiting, phishing e intrusiones internas/externas (firewalls) en los sistemas informáticos de las compañías. De igual manera, las empresas deben asegurarse de que su software de seguridad esté activo y reciba actualizaciones periódicas.</p> <p>En el caso de los sistemas automatizados y equipos de cómputo, se deben utilizar cuentas individuales que exijan un cambio periódico de la contraseña. Con el fin de proteger la confidencialidad, integridad y disposición de la información, la empresa debe tener políticas, procedimientos y normas de tecnología de informática establecidas, que se deben comunicar mediante un programa de capacitación, para todos los empleados que manejan equipos de cómputo y sistemas que incluya temas para prevenir ataques a través de la ingeniería social y todas aquellas amenazas a los que están expuestos (malware, baiting, phishing, etcétera). Las empresas que permiten a sus empleados conectarse de forma remota a una red, deben emplear tecnologías seguras, como redes privadas virtuales (VPN), para permitir que los empleados accedan a la intranet de la empresa de forma segura cuando se encuentran fuera de la oficina, así como procedimientos diseñados para evitar el acceso remoto de usuarios no autorizados.</p> <p>Por lo anterior, deben existir procedimientos escritos e infraestructura para proteger al Corporativo del Parque Industrial contra pérdidas, robo, fuga, hackeo y/o secuestro de información, esto incluye el procedimiento para la recuperación (o reemplazo) de los sistemas y/o datos de Tecnologías de la Información, así como un sistema o software establecido para identificar el abuso de los sistemas, detectar acceso inapropiado, manipulación indebida o alteración de los datos comerciales y del negocio, así como un procedimiento escrito para la aplicación de medidas disciplinarias apropiadas a todos los infractores. El acceso a los sistemas de Tecnologías de la Información debe protegerse contra la infiltración mediante el uso de contraseñas seguras, que incluyan frases u otras formas de autenticación. Los usuarios de dichos sistemas de Tecnologías de la Información deben salvaguardar y no compartir sus claves de accesos o contraseñas. Toda la infraestructura de Tecnologías de la información debe estar protegida físicamente contra el acceso no autorizado.</p>	

Respuesta:	Notas Explicativas:
	<p>Anexar el procedimiento para la recuperación que respalde y garantice la seguridad de su información, además de protegerla de posibles pérdidas. Asegúrese de incluir los siguientes puntos:</p> <ol style="list-style-type: none"> <li>I. Señalar la frecuencia con que se llevan a cabo las copias de respaldo.</li> <li>II. Quién tiene acceso a las mismas y quién autoriza la recuperación de la información.</li> <li>III. Indicar que tipo de pruebas realiza y cada cuando para verificar la seguridad de la red, los sistemas y la infraestructura.</li> <li>IV. Mencionar si para realizar este tipo de pruebas o escaneos de vulnerabilidad, lo hace a través de un software, un tercero o proveedor y, en su caso indique el nombre o razón social.</li> <li>V. En caso de encontrar vulnerabilidades, describa las acciones correctivas que deben implementarse.</li> <li>VI. Indicar si comparte información sobre las amenazas a la seguridad cibernética con sus socios comerciales que participan dentro de su cadena de suministro (por ejemplo: comunicados, boletines, correos electrónicos, etcétera).</li> <li>VII. Los sistemas deben estar protegidos bajo contraseñas y con frecuencia deben ser modificadas, indique el procedimiento para cambiarlas.</li> <li>VIII. Señalar si existen políticas de seguridad de la información para su protección.</li> <li>IX. Debe existir un sistema para detectar e identificar el abuso, intrusión o acceso de personas no autorizadas a sus sistemas, y/o datos de Tecnologías de la Información, así como el abuso de las políticas y procedimientos establecidos por la empresa, incluido el acceso indebido a sistemas internos, sitios web externos y la manipulación o alteración de datos comerciales por parte de empleados o contratistas.</li> <li>X. Todos los infractores deben estar sujetos a la aplicación de medidas disciplinarias, por lo anterior, indique los sistemas y políticas de políticas de seguridad de Tecnologías de la Información.</li> </ol>

	<p>Las políticas y los procedimientos de Tecnologías de la Información y seguridad cibernética deben revisarse anualmente y actualizarse derivado de algún ataque o de acuerdo a situaciones que puedan poner en riesgo los sistemas de la empresa.</p> <p>Describir las medidas de seguridad que utiliza para permitir a sus empleados conectarse de forma remota a una red (VPN), para permitir que los empleados accedan a la intranet de la empresa de forma remota cuando se encuentran fuera de la oficina.</p> <p>En caso de permitir que los empleados usen dispositivos personales para realizar el trabajo de la empresa, dichos dispositivos deben cumplir con las políticas y procedimientos de seguridad cibernética de la empresa, las actualizaciones de seguridad deben ser periódicas y contar con un método para acceder de forma segura a la red de la empresa.</p> <p>Señalar si los socios comerciales tienen acceso a los sistemas informáticos del Parque Industrial. En su caso, indique qué programas y cómo controlan el acceso a los mismos.</p> <p>Indicar si el equipo de cómputo cuenta con un sistema de respaldo de suministro eléctrico que permita la continuidad del negocio.</p> <p>Los procedimientos referentes al respaldo de la información de la empresa también deberán incluir:</p> <ol style="list-style-type: none"><li>I. Cómo y por cuánto tiempo se almacenan los datos (los datos deberían respaldarse una vez a la semana o según corresponda).</li><li>II. Plan de continuidad del negocio en caso de incidente y de cómo recuperar la información.</li><li>III. Frecuencia y localización de las copias de seguridad y de la información archivada.</li><li>IV. Si las copias de seguridad se almacenan en sitios alternativos a las instalaciones donde se encuentra el centro de proceso de datos.</li><li>V. Pruebas de la validez de la recuperación de los datos a partir de copias de seguridad.</li></ol>
--	--

	<p>Los procedimientos referentes al respaldo de la información del Parque Industrial también deberán incluir:</p> <ol style="list-style-type: none"> <li>I. Cómo y por cuánto tiempo se almacenan los datos (los datos deberían respaldarse una vez a la semana o según corresponda).</li> <li>II. Plan de continuidad del negocio en caso de incidente y de cómo recuperar la información.</li> <li>III. Frecuencia y localización de las copias de seguridad y de la información archivada.</li> <li>IV. Si las copias de seguridad se almacenan en sitios alternativos a las instalaciones donde se encuentra el centro de proceso de datos.</li> <li>V. Pruebas de la validez de la recuperación de los datos a partir de copias de seguridad.</li> </ol> <p>Los procedimientos referentes a la protección de la información del Parque Industrial también deberán incluir:</p> <ol style="list-style-type: none"> <li>I. Una política actualizada y documentada de protección de los sistemas informáticos del Parque Industrial de accesos no autorizados y destrucción deliberada o pérdida de la información. Todos los datos sensibles y confidenciales deben almacenarse en un formato cifrado o encriptado.</li> <li>II. Detallar si opera con sistemas múltiples (sedes/sitios) y cómo se controlan dichos sistemas.</li> <li>III. Quién es responsable de la protección del sistema informático del Parque Industrial (la responsabilidad no debería estar limitada a una persona, sino a varias, de forma que cada uno pueda controlar las acciones del resto).</li> <li>IV. El acceso de cada usuario debe asignarse a través de cuentas individuales y estar restringido según la descripción del trabajo o las tareas asignadas. Por lo anterior, describa cómo se conceden autorizaciones de acceso y nivel de acceso a los sistemas informáticos (el acceso a la información sensible deber estar limitado al personal autorizado a realizar modificaciones y uso de la información). El acceso autorizado debe monitorearse por parte del área responsable de concederlo, para verificar o en su caso reportar que el acceso a los sistemas confidenciales se basa en los requisitos del trabajo.</li> </ol>
--	--

	<p><b>V.</b> Indicar los elementos o formato que deben tener las contraseñas para el acceso a sistemas de Tecnologías de la Información y equipos de cómputo, frecuencia de cambios, si existen otros métodos de autenticación y quién o a qué área proporciona esas contraseñas.</p> <p><b>VI.</b> Indicar el nombre del cortafuego “firewall” y antivirus utilizados debiendo evidenciar que este software de seguridad está activo y recibe actualizaciones periódicas.</p> <p>Por lo anterior, las políticas y procedimientos de ciberseguridad deberían incluir medidas para prevenir el uso de productos tecnológicos falsificados o con licencias incorrectas.</p> <p>Todos los equipos de cómputo, medios electrónicos (discos duros, teléfonos celulares, etcétera) y hardware de Tecnologías de la Información que contengan información confidencial relacionada con el proceso de importación y exportación, deben contabilizarse mediante inventarios periódicos y contar con dicha evidencia. Cuando estos equipos tecnológicos se tengan que desechar, debe existir un procedimiento documentado que incluya como deben formatearse, desinfectarse o destruirse adecuadamente para evitar fuga de información.</p> <p><b>VII.</b> En caso de baja de personal, el acceso a equipos de cómputo, telecomunicaciones y red debe eliminarse al momento de la separación del empleado, esto incluye cuentas de correo electrónico, cuentas de accesos a sistemas, software, programas, etcétera.</p> <p><b>VIII.</b> Medidas previstas para tratar incidentes cuando el sistema se vea comprometido.</p>
<b>9. Capacitación en seguridad y concientización.</b>	
<p>Debe contar con un programa documentado de concientización sobre amenazas establecido diseñado y actualizado por el Comité de Seguridad para reconocer y crear conciencia sobre las amenazas de terroristas y contrabandistas en cada punto de la cadena de suministros. El programa de capacitación debe ser integral y cubrir todos los requisitos de seguridad del Programa Operador Económico Autorizado.</p> <p>Los empleados deben conocer los procedimientos establecidos del parque industrial para considerar una situación de riesgo y saber cómo denunciarla. Se debe brindar capacitación adicional a los empleados en las áreas con accesos y salidas de las instalaciones.</p>	

<b>9.1 Capacitación y concientización sobre amenazas.</b>	
<p>El Parque Industrial debe contar con un programa de capacitación y concientización de las políticas de seguridad en la cadena de suministros dirigido a todos sus empleados administrativos y de seguridad, adicionalmente, poner a su disposición material informativo sobre los procedimientos establecidos en el Parque Industrial para considerar una situación que amenace su seguridad y cómo denunciarla. Los registros de capacitación deben incluir la fecha de la capacitación, los nombres de los asistentes y los temas de la capacitación.</p> <p>De igual forma, se debe ofrecer capacitación al personal de seguridad conforme a sus funciones para ayudar a las empresas instaladas en el Parque Industrial a mantener la integridad de su carga, reconocer conspiraciones internas y proteger los controles de acceso.</p> <p>Aunado a los programas de capacitación en seguridad, se debe incluir un programa de concientización sobre consumo de alcohol y drogas. También, el personal debe estar capacitado en las políticas y procedimientos de ciberseguridad de la empresa, incluyendo el acceso al equipo de cómputo y sistemas mediante contraseñas o frases, el personal que opera y administra los sistemas de tecnología de seguridad debe recibir capacitación relacionada a su operación y mantenimiento, incluyendo autoformación a través de manuales operativos y otros métodos. Estos temas deben establecerse como parte de la inducción de nuevos empleados y mantener periódicamente programas de actualización.</p> <p>Los programas de capacitación deben fomentar la participación activa de los empleados en los controles y mecanismos de seguridad, así como mantener registros de todos los esfuerzos de capacitación que haya brindado el Corporativo del Parque Industrial y la relación de quienes participaron en ellos (videos, fotografías, minutas, listas de asistencia, intranet u otro sistema, material didáctico, presentaciones en PowerPoint, folletos, etcétera). Los registros de capacitación deben incluir la fecha de la capacitación, los nombres de los asistentes, los temas impartidos, además de tener medidas para verificar que la capacitación brindada cumplió con todos los objetivos de capacitación.</p>	
<b>Respuesta:</b>	<b>Notas Explicativas:</b>
	<p>Debe contar con un programa de capacitación en materia de seguridad y prevención en la cadena de suministros para todos los empleados. Explique brevemente en qué consiste y asegúrese de incluir lo siguiente:</p> <ol style="list-style-type: none"> <li>I. Breve descripción de los temas que se imparten en el programa.</li> <li>II. En qué momento se imparten (inducción, períodos específicos, etcétera).</li> <li>III. Periodicidad de las capacitaciones y en su caso, actualizaciones.</li> <li>IV. Indicar de qué forma se documenta la participación en las capacitaciones de seguridad en la cadena de suministros.</li> <li>V. Explicar cómo se fomenta la participación de los empleados en cuestiones de seguridad (videos, fotografías, minutas, listas de asistencias, intranet u otro sistema, material didáctico, presentaciones en PowerPoint, folletos, etcétera). Los registros deben incluir la fecha de la capacitación, los nombres de los asistentes, los temas impartidos, además de tener medidas para verificar que la capacitación brindada cumplió con todos los objetivos de la misma.</li> </ol>

	<p>La capacitación para realizar la revisión a los vehículos de carga, contenedores, remolques y/o semirremolques con fines agrícolas y de seguridad debe incluir los siguientes temas:</p> <ol style="list-style-type: none"> <li>I. Signos de compartimentos ocultos.</li> <li>II. Contrabando oculto en compartimentos naturales.</li> <li>III. Señales de contaminación por plagas.</li> <li>IV. Procedimientos a seguir si se encuentra algo durante una inspección del medio de transporte o si ocurre un incidente de seguridad durante el tránsito.</li> <li>V. La capacitación sobre revisiones agrícolas 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 (importaciones), por lo anterior, describa cómo cumple con las disposiciones señaladas por la SEMARNAT y la NOM-144 SEMARNAT-2017, en concordancia con la Norma Internacional de Medidas Fitosanitarias No.15 denominada "Reglamentación del embalaje de madera utilizado en el comercio internacional", las cuales emanan de la Organización de Naciones Unidas para la Alimentación y la Agricultura.</li> </ol>
<p><b>10. Manejo e investigación de incidentes.</b></p>	
<p>Deben existir procedimientos documentados para reportar e investigar incidentes de seguridad en la cadena de suministros, las acciones a tomar para evitar su recurrencia, así como notificarse al personal de seguridad, socios comerciales que pueden ser parte de la cadena de suministro afectada, especialista de seguridad o contacto del Programa Operador Económico Autorizado y/o demás autoridades competentes. Los procedimientos de reporte e investigación deben incluir la información de contacto o directorio actualizado que enumere los nombres y números de teléfono del personal que requiere notificación. La investigación y análisis de incidentes deberá estar documentada (expediente físico y/o electrónico), así como acciones correctivas para evitar que vuelva a ocurrir, mismas que deben implementarse a la brevedad.</p>	
<p><b>10.1 Reporte de anomalías y/o actividades sospechosas.</b></p>	
<p>En caso de detección de anomalías y/o actividades sospechosas relacionadas con la seguridad de la cadena de suministros y de conformidad con sus procesos logísticos (relacionadas al control de accesos, entrega, recepción y almacenamiento de mercancía, inspecciones de seguridad de los vehículos de carga y operadores de transporte, etcétera), estas deben notificarse al personal de seguridad del Centro de Monitoreo del Parque Industrial, socios comerciales que pueden ser parte de la cadena de suministro afectada, especialista de seguridad o contacto del Programa Operador Económico Autorizado y las autoridades competentes, llevando un registro de dichas anomalías y/o actividades inusuales.</p>	

Respuesta:	Notas Explicativas:
	<p>Describir el procedimiento para denunciar o reportar anomalías y/o actividades sospechosas y asegúrese de incluir lo siguiente:</p> <ol style="list-style-type: none"> <li>I. Quién es el responsable de reportar los incidentes.</li> <li>II. Detallar cómo determina con qué autoridad comunicarse en distintos supuestos o presunción de actividades sospechosas.</li> <li>III. Mencionar si lleva un registro del reporte de estas actividades y/o sospechas y describa brevemente en qué consiste.</li> </ol>
<b>10.2 Investigación y análisis.</b>	
<p>Deben existir un procedimiento escrito para denunciar o reportar anomalías y/o actividades sospechosas, así como para el análisis e investigación de incidentes relacionados con la seguridad de la carga que pudieran ocurrir al interior del parque industrial para determinar su causa, además de las acciones correctivas para evitar que vuelvan a ocurrir mismas que deben implementarse lo más pronto posible. La información derivada de la investigación conducida conjuntamente por el Centro de Monitoreo del Parque Industrial y por los responsables de seguridad de la empresa afectada, deberá documentarse y estar disponible en todo momento para las autoridades que así lo requieran.</p>	
Respuesta:	Notas Explicativas:
	<p>Describir el procedimiento documentado para iniciar una investigación en caso de ocurrir algún incidente relacionado con la seguridad de la carga y asegúrese de incluir lo siguiente:</p> <ol style="list-style-type: none"> <li>I. Responsable de llevar a cabo la investigación.</li> <li>II. Documentación que integra el expediente de la investigación del incidente de seguridad.</li> </ol> <p>Los documentos en el expediente derivado de la investigación, deben incluir al menos lo siguiente:</p> <ol style="list-style-type: none"> <li>I. Información general del embarque, orden de servicio.</li> <li>II. Solicitud de transporte; confirmación de medio de transporte; identificación del operador de transporte (registros de acceso, salida, registro de las inspecciones de seguridad, etcétera).</li> <li>III. Formatos de Inspección de medios de transporte; órdenes de salida; registros de recolección, entrega y recepción de mercancía de comercio exterior.</li> <li>IV. Videos de los sistemas de alarma y de circuito cerrado de televisión y video vigilancia.</li> <li>V. Documentación generada por y para socios comerciales y autoridades aduaneras.</li> <li>VI. Reporte de seguimiento y monitoreo de la unidad (rastreo del GPS).</li> </ol>