



SECTOR DE FABRICACIÓN CRÍTICA: Introducción al Mercado Gris



Esta hoja informativa informa a los lectores del continuo aumento del mercado gris y de cómo los componentes del mismo pueden afectar a las infraestructuras críticas nacionales. Este documento también presenta qué es el mercado gris, los tipos más comunes de componentes del mercado gris y por qué son problemáticos desde el punto de vista de la seguridad nacional.

¿QUÉ ES EL MERCADO GRIS?

Existen tres formas de mercado: el mercado blanco, el mercado gris y el mercado negro. Todos ellos plantean riesgos importantes, ya que podrían comprometer la información del comprador y de quienes se vean afectados por el uso de estos materiales. El mercado gris, o mercado intermedio, es un mercado no oficial que proporciona acceso a vendedores y compradores a través de canales no autorizados, aquellos que no están afiliados a la marca o a los fabricantes de componentes originales (OCM, por sus siglas en inglés). El proceso del mercado gris también se conoce como "importaciones paralelas".

¿QUÉ SON LOS MATERIALES DEL MERCADO GRIS? ¿CUÁLES SON LAS CAUSAS DEL MERCADO GRIS?

Los materiales del mercado gris son productos o componentes que se venden legalmente pero fuera del permiso de la marca y de los canales de distribución autorizados. Los canales y fabricantes autorizados son los asociados a la marca o al OCM. Todos los canales sin conexión con la marca o con el OCM se consideran canales de distribución no autorizados. Las existencias del mercado gris puede incluir piezas obsoletas o asignadas y productos de marca desviados a este mercado y que no pueden recibir soporte a través de su marca original autorizada, lo que puede causar problemas con las garantías y el soporte técnico. Además, los materiales del mercado gris pueden anunciarse como nuevos y auténticos pero, en cambio, son usados, reacondicionados o incluso falsificados.

Entre los materiales comunes del mercado gris se incluyen:

- Componentes electrónicos (memorias USB, sistemas domésticos/de alarma inteligentes, microchips [por ejemplo, circuitos integrados])
- Hardware informático, de seguridad y de red
- Materiales de construcción y otros metales en bruto (por ejemplo, aluminio y, sobre todo, acero, fabricados para fabricar tuercas, pernos, tornillos, vigas y otros materiales)

Los materiales del mercado gris pueden ponerse en circulación mediante:

- Las propias marcas cuando venden existencias antiguas.
- Terceros en la cadena de distribución (por ejemplo, minoristas o distribuidores que venden existencias antiguas).
- Empresas externas que venden imitaciones más baratas, pero funcionales, de productos comunes.

¿POR QUÉ LOS MATERIALES DEL MERCADO GRIS SON PROBLEMÁTICOS?

Los materiales del mercado gris pueden entrar en la cadena de suministro por numerosos puntos, lo que dificulta el rastreo de su origen y proveedor original. Los componentes y materiales comprados y vendidos en este mercado de segunda mano pueden crear riesgos inaceptables y peligrosos para todos los implicados.

Los riesgos de los componentes del mercado gris incluyen:

- Problemas de responsabilidad y seguridad: teniendo en cuenta la mayor probabilidad de abastecerse de componentes reacondicionados, defectuosos o incluso obsoletos o falsificados, los materiales del mercado gris aumentan el riesgo de accidente o falla debido a la calidad o fiabilidad del componente.
- Componentes mal etiquetados: algunos productos del mercado gris pueden estar mal etiquetados accidental o intencionalmente. Sin la posibilidad de rastrear o comprobar su originalidad, resulta imposible saber si el componente es auténtico o no.
- Garantías inválidas: a menudo, los productos del mercado gris no tienen garantía válida ni acuerdos de servicio. Varios fabricantes invalidan las garantías de las piezas que no pasan por los canales debidamente autorizados.

¿CÓMO AFECTA EL MERCADO GRIS AL SECTOR DE FABRICACIÓN CRÍTICA?

La seguridad de la cadena de suministro es vital para ofrecer productos y servicios trazables, genuinos y garantizados. Es imprescindible garantizar que los vendedores y proveedores cumplen los requisitos regulatorios.¹ Cuando se produce un incidente en la cadena de suministro, todos sufren: compradores, proveedores y consumidores. Los materiales del mercado gris en la fabricación crítica ponen en peligro el funcionamiento y la funcionalidad continuos de las infraestructuras críticas. Los propietarios y operadores de fabricación crítica deben conocer los riesgos de los materiales y componentes del mercado gris, ya que suponen una amenaza mucho mayor. Al tratar con materiales y componentes del mercado gris en un entorno de fabricación crítica surgen varios problemas.

- Problemas de ciberseguridad: conectar componentes a la red de una instalación puede introducir malware, spyware u otros programas dañinos.
- Problemas de producción: el uso de piezas del mercado gris puede presentar fallas o imperfecciones en los productos finales (por ejemplo, un tornillo del mercado gris puede fallar y provocar el mal funcionamiento del motor de un avión).
- Problemas de reputación: las fallas debidas al uso de materiales del mercado gris pueden dañar irreparablemente a una empresa o marca, especialmente si esa falla provoca lesiones o la pérdida de vidas humanas.
- Problemas de seguridad nacional: un componente o producto final fabricado con materiales del mercado gris puede pasar de un sector de infraestructuras críticas a otro, lo que aumenta el riesgo nacional.

¿CÓMO EVITAR LOS MATERIALES DEL MERCADO GRIS?

La forma más confiable de evitar los materiales del mercado gris y obtener productos auténticos es comprar directamente a fabricantes autorizados o distribuidores autorizados, los relacionados con la marca o con el OCM. Evitar por completo los materiales del mercado gris es la mejor y más segura opción. Mantenerse al día sobre las especificaciones de información de productos autorizados (por ejemplo, números de serie, números específicos de unidades de mantenimiento de existencias [SKU, por sus siglas en inglés] y materiales de construcción autorizados) es una forma en que los propietarios y operadores de fabricación crítica pueden reducir el riesgo de utilizar materiales sospechosos del mercado gris.

Para evitar los peligros de los materiales del mercado gris, es fundamental:

- Comprar directamente a fabricantes o distribuidores autorizados.
- Investigar y establecer relaciones con proveedores de confianza.
- Obtener los números de serie de los componentes.
- Reportar a los proveedores o distribuidores dudosos a la oficina de compras de la organización y a los fabricantes y distribuidores oficiales.

EJEMPLO DE ESTUDIO DE CASO PERTINENTE

El Comité de Servicios Armados del Senado (Senate Armed Services Committee, SASC) inició una investigación sobre piezas electrónicas falsificadas en la cadena de suministro del Departamento de Defensa entre 2009 y 2011. Varias de estas piezas procedían de diversos puntos de reventa de Estados Unidos, Reino Unido y Canadá. Los investigadores señalaron a China como fuente de los componentes electrónicos falsificados. La investigación descubrió presuntas piezas falsificadas en computadoras de misión para misiles de la Agencia Antimisiles de Defensa (Missile Defense Agency, MDA) y visores térmicos de armas entregados al Ejército y en aviones militares. Se identificaron 1,800 casos de falsificación y menos de un millón de piezas sospechosas en total. Posteriormente, se prohibió la entrada en China al personal del SASC. Todos los materiales, componentes y piezas electrónicas deben examinarse para garantizar que son productos de distribuidores y proveedores autorizados o franquiciados dentro de la cadena de suministro. Este proceso de verificación y autenticación ofrece la máxima confianza en la autenticidad y el menor riesgo de adquirir materiales del mercado gris y falsificaciones.²

PARA MÁS INFORMACIÓN SOBRE EL SECTOR DE FABRICACIÓN CRÍTICA

Póngase en contacto con el Equipo de Gestión del Sector de Fabricación Crítica en CriticalManufacturingSector@cisa.dhs.gov o visite cisa.gov/critical-manufacturing-sector para saber más.

¹ Los requisitos regulatorios de la cadena de suministro incluyen, de manera enunciativa mas no limitativa, la normativa sobre comercio internacional; las normas medioambientales, sociales y de gobierno (ESG, por sus siglas en inglés); la normativa sobre seguridad y calidad de los productos; la normativa sobre privacidad y seguridad de los datos; y la normativa contra la corrupción y el soborno.

² Abesamis, C. and Leblanc, M. (2015) NASA Counterfeit Parts Awareness and Inspection [diapositivas 23 y 24 de PowerPoint]. Obtenido de la copia en versión PDF de NASA Counterfeits Parts Awareness and Inspection.