Contacto

PSTI de Reino Unido

Applus+ Laboratories, líder global en evaluaciones de ciberseguridad, se complace en anunciar un nuevo servicio diseñado específicamente para los fabricantes y distribuidores que busquen cumplir con el Anexo 1 de la regulación de Seguridad de Productos y Telecomunicaciones del Reino Unido (UK-PSTI).

UK PSTI, una nueva regulación del Reino Unido para productos conectados

Aunque la nueva Regulación de Ciberseguridad para Dispositivos de Consumo Conectados del Reino Unido se basa en el cumplimiento propio del proveedor, **obtener un certificado de un tercero sigue siendo una opción recomendable.** Applus+ Laboratories ofrece varias opciones para los proveedores que buscan una prueba independiente de cumplimiento.

¿Qué es el UK PSTI (Seguridad de Productos e Infraestructura de Telecomunicaciones)?

El Régimen de Seguridad de Productos del UK PSTI (Product Security and Telecommunications Infrastructure) es un marco legal destinado a exigir requisitos de seguridad para los productos IoT vendidos en el Reino Unido.

El marco legal del PSTI se compone de dos partes que se resumen a continuación:

El 29 de abril de 2024, las regulaciones del Acta de Seguridad de Productos e Infraestructura de Telecomunicaciones **entraron en vigor de manera inmediata** y no hay ninguna disposición en el régimen que excluya productos que ya estén en el mercado del Reino Unido.

¿Qué productos se ven afectados por el UK PSTI y qué requisitos están al alcance?

El régimen del UK PSTI abarca una amplia gama de productos. Desde termostatos inteligentes hasta rastreadores de actividad física, los dispositivos cotidianos ahora son parte integral de la conversación sobre seguridad. Para algunas empresas de TI, este nivel de ciberseguridad es algo conocido, superado desde hace tiempo. Pero para otras es un territorio inexplorado, lo que requiere una evaluación exhaustiva de sus prácticas actuales y la identificación de los cambios necesarios para garantizar el cumplimiento.

Los fabricantes deben implementar las medidas de seguridad mínimas definidas en el Anexo 1 y la regulación se basa en un enfoque de autoevaluación. Estas medidas de seguridad se relacionan con tres elementos principales:

Contraseñas

Los fabricantes deben asegurarse de que las contraseñas de los productos tengan una seguridad mínima, como ser una sólo por dispositivo o que hayan sido establecidas por el usuario, evitando patrones adivinables o que contenga información disponible públicamente.

Información sobre cómo reportar problemas de seguridad

Los fabricantes deben proporcionar vías de contacto claras para que los usuarios puedan informar sobre cuestiones de seguridad, con garantías de reconocimiento y actualizaciones de estado, que puedan ser accesibles sin requisitos de datos personales.

Información sobre períodos mínimos de actualización de seguridad

Los fabricantes deben publicar períodos de soporte definidos para actualizaciones de seguridad, asegurando la accesibilidad y transparencia, sin que sea necesaria una solicitud previa, en un lenguaje comprensible y sin requerimientos de información personal.

Autoevaluación y certificación de terceros para el UK PSTI

Bajo esta nueva regulación, no existen organismos de certificación obligatorios que verifiquen activamente el cumplimiento. La responsabilidad recae completamente en los

proveedores. Sin embargo, obtener una prueba de cumplimiento emitida por una tercera parte sigue siendo una opción más que prudente. La validación independiente realizada por terceros añade credibilidad.

Para los fabricantes sin equipos internos de ciberseguridad, la certificación por parte de terceros simplifica el proceso. Las empresas más pequeñas pueden resolver asuntos complejos de manera más efectiva. Además, mostrar un certificado indica compromiso con la seguridad, fomentando la confianza del consumidor. Esta se refuerza cuando los consumidores ven que una evaluación independiente ha validado un producto.

A medida que otros países siguen con regulaciones similares, este enfoque proactivo se vuelve esencial para los proveedores que venden productos en el mercado global.

Soluciones de servicio de conformidad de Applus+ Laboratories para el cumplimiento del UK PSTI

Applus+ Laboratories ofrece varias soluciones de servicio para el cumplimiento del UK PSTI:

Certificado enfocado en PSTI

Applus+ Laboratories revisará y analizará la documentación proporcionada y emitirá un informe que permitirá al fabricante demostrar el cumplimiento propio de la regulación. Opcionalmente, Applus+ Laboratories también puede proporcionar un Certificado de Cumplimiento (CoC), lo que fortalecerá la confianza del cliente en caso de que necesiten demostrar a terceros el cumplimiento de esta regulación. Esto permitirá a los clientes demostrar el cumplimiento pero también identificar posibles brechas, ayudándolos en su camino para cumplir con los requisitos de seguridad del UK-PSTI. Nuestro análisis imparcial, realizado por los principales expertos en regulaciones actuales de ciberseguridad, asegura una evaluación exhaustiva y precisa.

Nuestro servicio especializado proporciona una **evaluación completa** de los requisitos de seguridad descritos en el Anexo 1 de la regulación UK-PSTI. Esta evaluación asegura que los fabricantes puedan utilizar los resultados como evidencia para demostrar el cumplimiento de los requisitos de seguridad establecidos en la regulación UK-PSTI. Con Applus+ Laboratories, los fabricantes y distribuidores pueden evaluar sus áreas regulatorias clave de manera eficiente y efectiva por una entidad independiente y con experiencia, lo que les permitirá conocer su estado y posibles brechas con anticipación.

Evaluación completa ETSI EN 303 645

Para aquellos que apuntan más alto, existe la opción de realizar una evaluación contra la norma completa ETSI EN 303 645. Ten en cuenta que si su producto ya cumple con ETSI 303 645, se considera que cumple con las regulaciones de ciberseguridad del UK-

PSTI. Applus+ Laboratories tiene la acreditación ISO/IEC 17025 con ETSI 303 645 como Laboratorio de Evaluación.

Esquema PSA Certified Nivel 1

PSA Certified es un esquema de certificación liderado por la industria para la ciberseguridad de productos IoT. La marca de Nivel 1 se alinea con las principales directrices globales para la seguridad de dispositivos de consumo conectados, mapeando requisitos de varios estándares, incluyendo ETSI EN 303 645, NIST 8259A, PSTI, Ley Estatal de California SB-327, Matter e ioXt.

¡Contáctanos para garantizar el cumplimiento de la regulación PSTI ya en vigor!

Confía en Applus+ Laboratories para guiarte a través del panorama de ciberseguridad del UK-PSTI, proporcionando la experiencia necesaria para ayudarte a conseguir tus objetivos de cumplimiento sin problemas.

¡Contáctanos hoy para proteger tus dispositivos de consumo y mejorar la confianza en un mundo conectado o solicita una propuesta!