LISTA DE VERIFICACIÓN PARA LOS MINORISTAS DE PRODUCTOS Y SERVICIOS CONECTADOS COMERCIALIZADOS PARA NIÑOS O PARA NIÑOS

CONSUMERS INTERNATIONAL
AUNANDO ESFUERZOS PARA EL CAMBIO

Los juguetes y productos que se conectan a Internet son cada vez más populares entre los niños y sus padres. Sin embargo, sin la debida protección y seguridad, los datos recopilados por cosas como juguetes inteligentes, relojes o monitores para bebés conectados pueden compartirse, visualizarse y usarse de maneras que exponen a los niños a riesgos.

Los estándares claros y la certificación están en proceso de desarrollo, pero actualmente, es difícil para los minoristas de productos para niños conectados saber cómo garantizar que los productos conectados que usted almacena sean seguros y no utilicen los datos de manera inapropiada.

Esta lista de verificación de seguridad y privacidad ha sido desarrollada para ayudarlo a examinar proveedores potenciales en base a un conjunto de criterios simples para garantizar que los juguetes que almacenan cumplan con un estándar básico de seguridad para su usuario final. No pretende reemplazar a las normas obligatorias o voluntarias que están en desarrollo, pero es una herramienta útil mientras están en desarrollo.

La lista de verificación ha sido informada por expertos técnicos en seguridad del sistema, pruebas de intrusión y por miembros de Consumers International que trabajan en estándares digitales, seguridad cibernética y seguridad del producto, principios para Internet de las cosas y códigos de prácticas gubernamentales nacionales[1].

SEGURIDAD		
1	¿Hay algo en Internet que esté de alguna manera conectado con el dispositivo inteligente • que cumpla con el estándar de verificación de seguridad de la aplicación OWASP2, artículos V1-V20, en el nivel 1 o superior? • han establecido métodos para incorporar cualquier actualización a la norma de manera oportuna?	☐ ☐
2	¿Los usuarios deben • agregar un método de autenticación apropiado, como una contraseña fuerte única3, a sus cuentas cuando se crean por primera vez? • en caso afirmativo, ¿el método ofrecido limita el riesgo para el usuario final teniendo en cuenta la edad del usuario final y el método más eficaz para proteger su seguridad?	☐ ☐
3	¿Ha publicado el proveedor de dispositivos inteligentes • un programa de divulgación responsable, con un punto de contacto designado, para que los investigadores de seguridad informen sobre los problemas de seguridad? • se ha comprometido a solucionar los problemas de seguridad que exponen los datos del usuario u otra información dentro de los 90 días de recibir un informe?	☐ ☐
4	¿Han adoptado todas las aplicaciones móviles conectadas al dispositivo inteligente procedimientos para • detectar de manera proactiva y remediar los riesgos de OWASP Mobile Application Security? • actualiza las aplicaciones móviles afectadas de manera oportuna?	☐ ☐
5	¿La infraestructura del servidor, que admite dispositivos inteligentes y aplicaciones, se comunica o interactúa a través de Internet, protegida contra las amenazas como se describe en el Centro de Puntos de Referencia de Seguridad de Internet?	☐

DERECHOS DEL CONSUMIDOR

6	Para productos donde las vulnerabilidades críticas representan una amenaza importante para la funcionalidad o seguridad del producto y otros dispositivos en la red y no se pueden resolver en 90 días a través de una actualización de software o firmware, ¿usted está: • retirando inmediatamente los productos de la venta? • avisar a los propietarios existentes y permitirles devolver el producto? • ¿proporciona una compensación a los propietarios que salen o les permite cambiar el producto por una versión segura?	☐ ☐ ☐
7	¿Ha explicado y dejado en claro por adelantado todas las actualizaciones de software?	☐
8	¿Está brindando soporte a productos al final de su vida brindando actualizaciones de software del producto relacionadas con cuestiones de seguridad durante un mínimo de tres años (desde la fecha en que se vende el producto al usuario)?	☐

CIFRADO

9	¿Todas las conexiones alámbricas e inalámbricas al dispositivo, como Wi-Fi, Bluetooth, Zigbee, Z-Wave, siguen la guía criptográfica de administración de claves específica de la aplicación?	☐
10	¿Están todos los datos en tránsito o en reposo sujetos a encriptación fuerte como TLS 1.2 / 1.3, SSH 2, VPN / IPSec, PKCS # 1 v 2.x, Sintaxis de mensaje criptográfico (S / MIME)?	☐
11	¿Están encriptados todos los datos a los que acceden terceros?	☐
12	¿El hardware, el firmware y el software que se encuentran en el dispositivo inteligente emplean un entorno de ejecución de confianza, almacenamiento seguro para datos confidenciales como claves criptográficas y una fuente de entropía pseudoaleatoria para generar operaciones criptográficas?	☐

PRIVACIDAD DE DATOS

13	El producto • ¿tiene una política de privacidad y términos y condiciones de fácil acceso, escritos en un lenguaje que sea fácil de entender y apropiado para la persona que usa el dispositivo o servicio? • ¿informa a los usuarios sobre los cambios en los términos y condiciones o las políticas de privacidad por adelantado y se les dará la oportunidad de retirarse del contrato? • ¿garantiza que toda la conectividad, configuración y opciones no necesarias para entregar el servicio en cualquier producto sigan la privacidad según los estándares de diseño, y los usuarios soliciten su consentimiento para la recopilación, transmisión y distribución de datos; y cuando los datos se utilizan con fines de comercialización? • ¿permite a los usuarios acceder y eliminar fácilmente sus datos y su cuenta? • ¿borra automáticamente los datos después de un período máximo establecido para la retención de datos?	☐ ☐ ☐ ☐ ☐

1 Consumer Reports, Estándar Digital https://www.consumerreports.org/privacy/setting-standards-for-digital-privacy/
Asegurando nuestra confianza, 2017, ANEC, BEUC, Consumers International, ICRT http://www.consumersinternational.org/news-resources/news/releases/consumers-international-launches-joint-iot-principles/
Seguro por diseño: mejorar la seguridad cibernética de Internet de los consumidores, 2018 DCMS (Reino Unido) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf
Ciberseguridad para productos conectados, 2018, ANEC y BEUC. Documento de posicionamiento: http://www.anec.eu/images/Publications/position-papers/Digital/ANEC-DIGITAL-2018-G-001final.pdf

2 OWASP, Application Security Verification Standard Project

3 Las contraseñas seguras necesitan sistemas que no permitan al usuario cambiar la contraseña de la cuenta sin la contraseña original, tener un almacenamiento de contraseña adecuado (por ejemplo, utilizar hash y un método de encriptación fuerte) y proporcionar un indicador claro de contraseña (es decir, mayúsculas y minúsculas, dígitos, Símbolos, uso de caracteres ASCII y UNICODE y sin contraseñas comunes de un diccionario