ESTUDIO DE LA CIBERSEGURIDAD

JUGUETES CONECTADOS

Campaña Navidad 2024

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

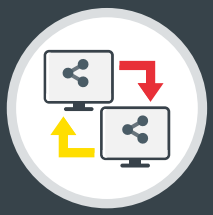
ESTUDIO DEL ESTADO DE LA CIBERSEGURIDAD EN JUGUETES CONECTADOS

JUGUETES INTELIGENTES

Cada vez es más común encontrar **juguetes interactivos** ofreciendo nuevas formas de entretenimiento. Además, gracias a la evolución tecnológica, estos juguetes tienen en la actualidad una gran relevancia y presencia en el mercado.

Muchos de los denominados como ***"Smart toys"*** o **"Juguetes inteligentes"**, disponen de capacidades avanzadas, tales como:

CONEXIÓN A INTERNET



COMPARTICIÓN DE INFORMACIÓN ENTRE DISPOSITIVOS

INTERACCIÓN CON ACTUADORES Y SENSORES

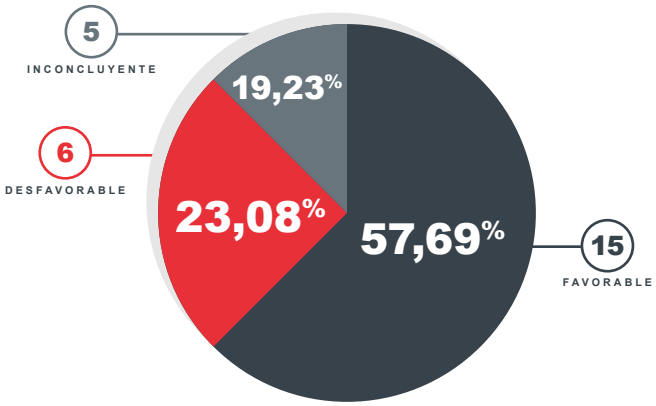
INTEGRACIÓN DE CÁMARAS DE VÍDEO Y MICRÓFONOS

Dado que van a ser dirigidos a un público infantil, la ciberseguridad en estos dispositivos es **crucial**, y al ser dispositivos muy variados tienen diferentes tipos de amenazas sobre sus distintos componentes y capacidades.

En el presente estudio, **INCIBE ha analizado 26 juguetes inteligentes** con capacidad de manejar datos del usuario, grabar vídeo o audio, conexión Bluetooth o Wi-Fi o aplicación móvil para el manejo del dispositivo; evaluando sus puntos fuertes y aspectos de mejora y emitiendo recomendaciones para fabricantes y consumidores.

ESTADÍSTICAS **GENERALES**

26 Juguetes conectados evaluados



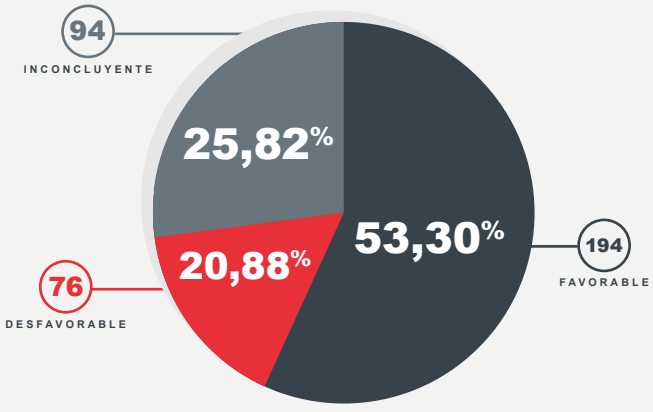
Una pequeña parte de los juguetes, **un total de cinco**, arrojan resultados que se dan como inconcluyentes, debido fundamentalmente a la falta de información pública que los fabricantes muestran acerca de las configuraciones que disponen, componentes y versiones *software*, tratamientos de datos personales, directivas y normas aplicadas, etcétera.

La **mayoría de los dispositivos analizados** obtienen resultados mayoritariamente favorables en las pruebas realizadas. Representan un avance hacia mejores estándares de ciberseguridad y la confianza digital en el usuario. Estos dispositivos presentan niveles de seguridad aceptables según los criterios evaluados, destacándose como los más confiables dentro del grupo.

Seis dispositivos obtienen resultados mayoritariamente desfavorables en las pruebas realizadas: No cumplen con los requisitos mínimos de ciberseguridad. Suponen un riesgo directo para los usuarios finales y el ecosistema conectado. Podrían convertirse en puntos de entrada para ciberataques.

La mayoría de las pruebas con **resultado favorable**, aunque solo algo más de la mitad. Nivel razonable de cumplimiento con los criterios establecidos en cuanto al análisis del panorama actual. No obstante, este porcentaje es solo ligeramente superior a la mitad. Evidencia debilidades importantes en un quinto de las pruebas marcadas como “desfavorable”.

Un cuarto de las pruebas no se pueden determinar con certeza: Señalan una falta de datos y documentación técnica pública de los dispositivos. Es un indicador más de la necesidad de estrecha colaboración entre fabricantes y laboratorios y entidades evaluadoras.



364 Pruebas realizadas en total

RECOMENDACIONES PARA **USUARIOS Y FAMILIAS**

Se recomienda que las familias evalúen las funcionalidades, capacidades e información técnica de los productos y se aseguren de tener en cuenta las buenas prácticas de ciberseguridad en su uso, comunes a otros dispositivos informáticos, como por ejemplo: mantenerlos actualizados, utilizar contraseñas robustas y apagarlos cuando no se estén usando.

CONFIGURAR EL DISPOSITIVO DE MANERA SEGURA

Cambiar las contraseñas predeterminadas de los dispositivos conectados, utilizando siempre contraseñas robustas.

Usar siempre redes Wi-Fi de confianza. Evitar el uso de redes abiertas o inseguras que puedan facilitar el acceso no autorizado.

Asegurarse de que el dispositivo tenga habilitadas las interfaces de comunicación mínimas necesarias, desactivando por ejemplo características como el emparejamiento automático de Bluetooth.

BUENAS PRÁCTICAS EN EL USO DE JUGUETES INTELIGENTES Y CONECTADOS

Mantener los dispositivos actualizados: no cancelar o demorar las actualizaciones de software que emita el fabricante.

Apagar los dispositivos cuando no se estén utilizando.

Tapar u orientar la cámara del dispositivo para que no tenga visión directa de las estancias de la casa cuando no se esté usando.

SUPERVISAR EL USO DE LOS DISPOSITIVOS

Controlar y limitar el acceso de los dispositivos a Internet, especialmente en el caso de juguetes que permiten la comunicación remota.

Considera utilizar herramientas de control parental para gestionar el acceso a contenidos y la interacción con otros usuarios.

INVESTIGAR ANTES DE COMPRAR

Comprobar si el juguete tiene certificaciones o el fabricante está adherido a programas de ciberseguridad de sus productos.

Asegurar que el fabricante ofrece información pública sobre el producto, para conocer qué directivas cumple y qué medidas de seguridad (y ciberseguridad) aplica.

Leer y comprobar reseñas de otros consumidores.

TENER EN CUENTA LAS POLÍTICAS DE PRIVACIDAD

Antes de conectar el juguete a Internet, revisar detenidamente las políticas de privacidad para comprender qué datos se recopilan y cómo se protegen.

Comprobar que la información personal sea manejada adecuadamente y que se tenga la opción de solicitar y revocas los datos.

RECOMENDACIONES PARA
FABRICANTES Y DISTRIBUIDORES

Es clave que los fabricantes comiencen a implementar medidas para el cumplimiento y conformidad de sus productos con la Ley de Ciberresiliencia: adoptar la ciberseguridad desde el diseño, procedimientos para la notificación y parcheo de vulnerabilidades, incorporar configuraciones de ciberseguridad por defecto y medidas adecuadas para la protección de los datos y las comunicaciones.

MEJORAR LA SEGURIDAD POR DEFECTO

Deshabilitar servicios o protocolos innecesarios para minimizar vectores de ataque.

Incorporar funciones predeterminadas que brinden un nivel adecuado de seguridad desde el primer uso.

Detallar funciones de control parental para evitar un uso indebido e inseguro del dispositivo.

Implementar técnicas de desarrollo de software seguro.

Incorporar elementos fisicos que ayudan a proteger el dispositivo, como botones de apagado con corte de suministro eléctrico o mecanismos que cubran el objetivo de la cámara web cuando no se está usando.

COMUNICACIONES ROBUSTAS Y GESTIÓN SEGURA DE DATOS

Empleo de protocolos robustos en las comunicaciones.

Implementar medidas de cifrado tanto para la transmisión como para el almacenamiento de datos.

Proporcionar herramientas para que los usuarios puedan revisar, modificar o eliminar sus datos fácilmente.

FORTALECER LA TRANSPARENCIA

Proveer información clara, accesible y detallada sobre cómo se gestionan los datos de los usuarios.

Implementar interfaces intuitivas que permitan a los usuarios configurar fácilmente sus preferencias de privacidad y seguridad.

Diseñar manuales, guías de usuario y configuraciones de privacidad y seguridad que sean fáciles de entender para usuarios no técnicos.

CUMPLIMIENTO NORMATIVO Y ALINEACIÓN CON LA LEY DE CIBERRESILIENCIA (CRA):

Diseñar productos que cumplan con las normativas de privacidad y ciberseguridad vigentes y futuras.

Someter los dispositivos a evaluaciones de seguridad rigurosas antes de su lanzamiento al mercado.

Obtener certificaciones reconocidas que validen el cumplimiento de estándares internacionales en ciberseguridad.

Establecer canales de comunicación efectivos para notificar a los usuarios sobre incidentes y medidas correctivas.

ESTADÍSTICAS GENERALES
RESULTADOS POR JUGUETE

5 DISPOSITIVOS SUPERAN EL 75% DE PRUEBAS FAVORABLES

MAYOR SOLIDEZ EN CIBERSEGURIDAD

Diseño enfocado en la seguridad infantil

Equilibrio entre funciones avanzadas y medidas de seguridad robustas.

Reputación de los fabricantes. Priorizan la protección de los usuarios mediante estándares elevados y actualizaciones periódicas

Transparencia al usuario en cuanto a información recabada, tratamiento de datos y conocimiento de leyes y normativas a implementar.

Tecnologías y protocolos inherentemente seguros por diseño.

Variabilidad en cumplimiento: Disparidad en el porcentaje de pruebas válidas, indicando diferentes niveles de conformidad con los criterios evaluados.

POE (PRODUCTO OBJETIVO DE EVALUACIÓN)

5 DISPOSITIVOS NO SUPERAN EL 35% DE PRUEBAS FAVORABLES

DEBILIDADES O INCUMPLIMIENTOS SIGNIFICATIVOS

Tendencia general: La mayoría de los dispositivos se sitúan entre el 40% y el 75%, mostrando una tanto fortalezas y puntos fuertes como áreas críticas a resolver.

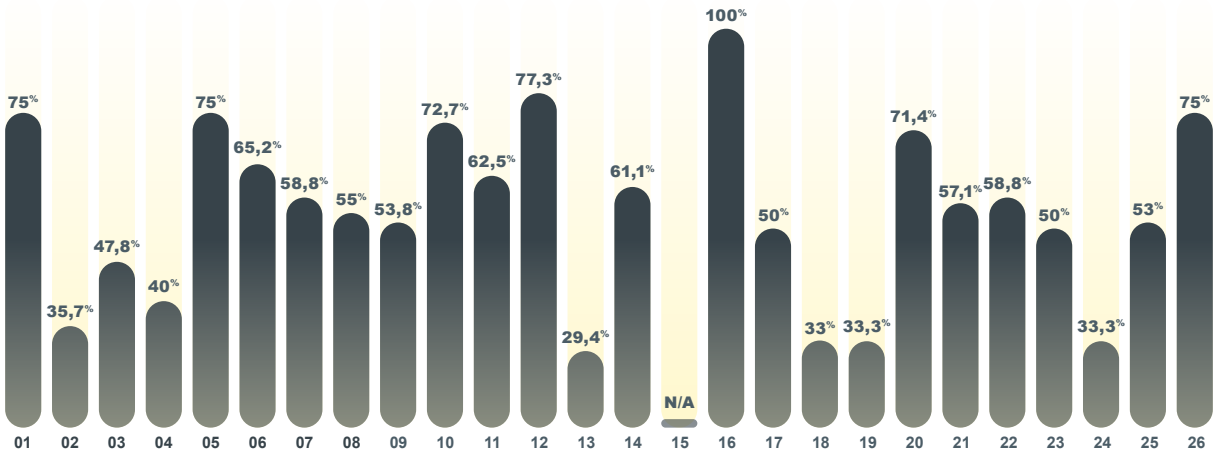
Falta de cifrado para datos sensibles, que expone a los usuarios a riesgos graves de intercepción de información.

Servicios innecesarios habilitados: presencia de servicios habilitados sin justificación funcional, con credenciales predeterminadas y/o de dominio público.

Uso de tecnologías obsoletas o inseguras, que deja a los dispositivos vulnerables a ataques bien documentados.

Falta de medidas para restringir el acceso ilegítimo.

Inadecuación frente a estándares modernos y futuras leyes y normas.



Porcentaje de pruebas favorables para cada juguete evaluado

ESTADÍSTICAS GENERALES
RESULTADOS VECTOR ANALIZADO

Porcentaje de pruebas favorables por cada vector analizado

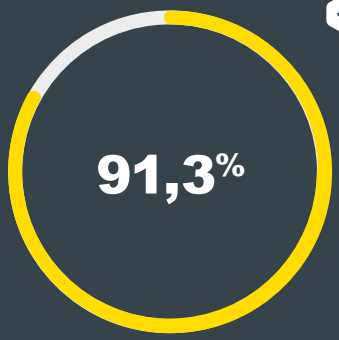
68,8%
ANÁLISIS DE VULNERABILIDADES
Estructura razonablemente resistente a vulnerabilidades conocidas y minimización de puertos y servicios innecesarios expuestos.

53,8%
COMUNICACIONES
Las medidas de seguridad en las comunicaciones y recolección de datos requieren fortalecimiento.

41,8%
ACTUALIZACIONES
Necesidad de mejorar los mecanismos de actualización de *firmware* y la periodicidad de los mismos.

19%
FIRMWARE
Graves riesgos relacionados con la integridad y seguridad del *firmware*.

Este vector es fundamental, compromisos en esta área pueden exponer todo el sistema.



INTERFACES FÍSICAS Y AÉREAS
Sólida protección frente a accesos no autorizados a conexiones físicas o inalámbricas.

81,9%
APLICACIÓN MÓVIL
Alto nivel de seguridad en las aplicaciones móviles asociadas.

19,7%
MÉTODOS DE AUTENTICACIÓN
Importantes carencias en la robustez de los sistemas que verifican la identidad de usuarios.

VECTORES MÁS SÓLIDOS
Interfaces físicas y aéreas y aplicaciones móviles complementarias.

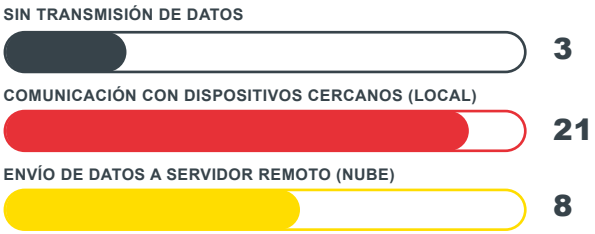
ÁREAS INTERMEDIAS
Análisis de vulnerabilidades, seguridad de las comunicaciones y mecanismos de actualización.

ÁREAS CRÍTICAS
Métodos de autenticación y seguridad del *firmware*.

ESTADÍSTICAS GENERALES
TRATAMIENTO DATOS SENSIBLES

El **envío de datos a la nube** mediante acceso remoto supone un riesgo de exposición si el cifrado o la autenticación son débiles. El tratamiento de datos se realiza por parte de externos.

La **comunicación local** a través de dispositivos cercanos reduce la dependencia de internet y la exposición global.

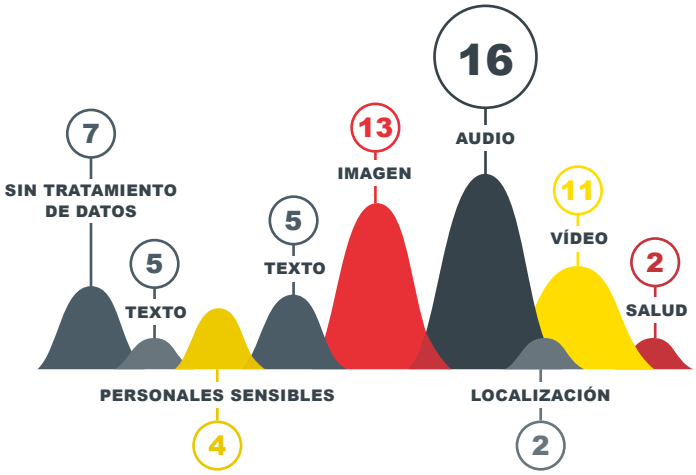


ALMACENAMIENTO DE DATOS

La **mayoría no almacena datos**, lo cual elimina riesgos asociados a la exposición de información.

En cuanto al tratamiento, existe una alta **recolección de datos privados críticos** como la imagen, vídeo y audio.

El tratamiento de **datos personales sensibles** como tarjetas de crédito, credenciales, datos de padres y niños, suponen unos datos menores.



ESTADÍSTICAS GENERALES
TECNOLOGÍAS DE CONECTIVIDAD

DIVERSIDAD DE TECNOLOGÍAS

Diferentes vectores de ataque potenciales.

TECNOLOGÍAS MÁS EMPLEADAS

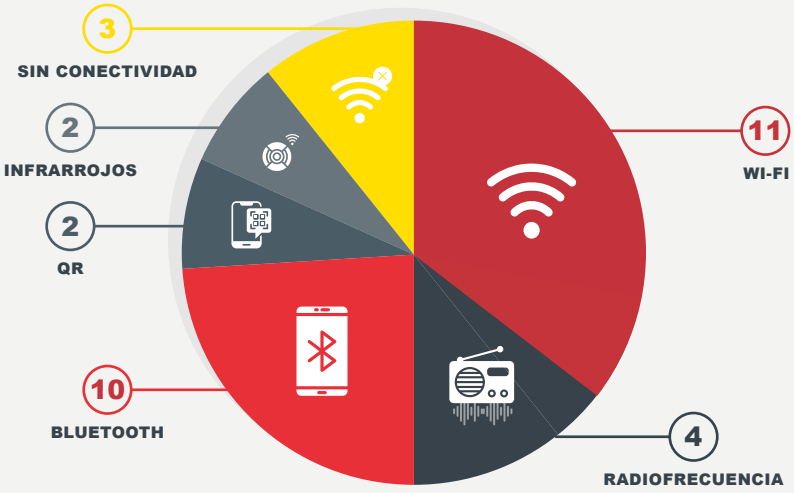
- Wi-Fi y Bluetooth.
- Conectividad inalámbrica es susceptible a ataques de interceptación, acceso no autorizado y manipulación remota

IMPACTO DE LAS TECNOLOGÍAS DE BAJA DISTANCIA

- Radiofrecuencia e infrarrojos presentan un riesgo menor.
- Pueden ser explotadas si la comunicación no está cifrada adecuadamente.
- La protección física y codificación de señales vitales.

DISPOSITIVOS SIN CONECTIVIDAD

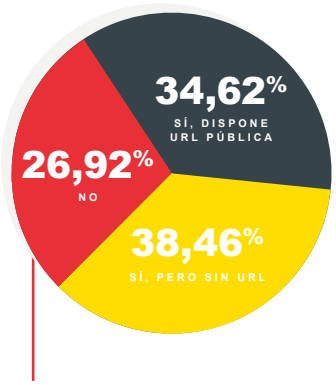
- Parecen más seguros, pero no deben ser ignorados.
- Indirectamente conectividad por control de aplicación de configuración y acceso.
- Las amenazas físicas o el acceso no autorizado pueden comprometer su funcionamiento o manipulación.



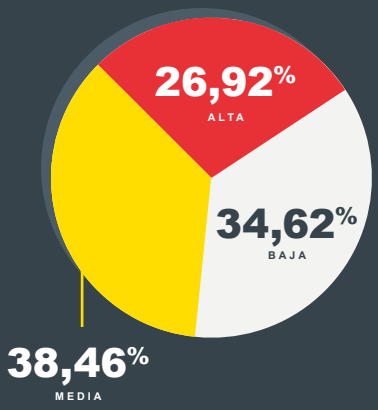
ESTADÍSTICAS GENERALES
ALINEAMIENTO CON CRA Y RGPD

DECLARACIÓN UE
DE CONFORMIDAD

Entorno al **75% disponen de una declaración UE** de conformidad. Transparencia de acceso a la información sobre su cumplimiento con las normativas. Sin embargo, el **38,46% no cumplen con lo requerido para la CRA**.



Solo presentan un marcado CE, sin información sobre las directivas aplicadas. Confianza ciega en el fabricante.



APLICABILIDAD
REQUISITOS ESENCIALES

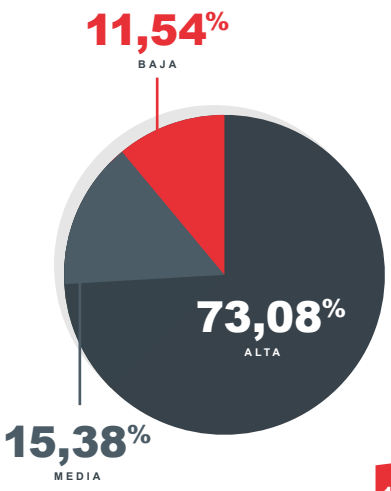
Cumplimiento y resiliencia, pero limitada con controles efectivos sobre vulnerabilidades e información pública clara sobre la notificación y manejo de vulnerabilidades, periodos de soporte y materiales.

Una mitad necesita mejoras, la otra falla completamente: Pruebas parcialmente adecuadas, pero falta de documentación pública de material y reportes. Fallos significativos en las pruebas de seguridad. Carencias en información pública y confianza digital.

TRANSPARENCIA
TRATAMIENTO DE DATOS

Confianza y acceso a información tratada: Alta transparencia general y acceso fácil a información clave sobre la seguridad, la privacidad y el manejo de datos.

Las **políticas de privacidad generalistas** no hablan del tratamiento de datos del juguete en concreto. No se hacen menciones directas a usuarios de la UE. La solicitud visualización y borrado de datos no es sencilla o está oculta.



ESTADÍSTICAS **GENERALES**

CONFIGURACIÓN Y OPERABILIDAD VÍA TELÉFONO MÓVIL

APLICACIÓN PROPIA:

Suelen ofrecer un mayor control sobre la funcionalidad y seguridad.

Si no están bien diseñadas, pueden incluir vulnerabilidades específicas que afecten la seguridad y los datos del usuario.

APLICACIÓN GENÉRICA:

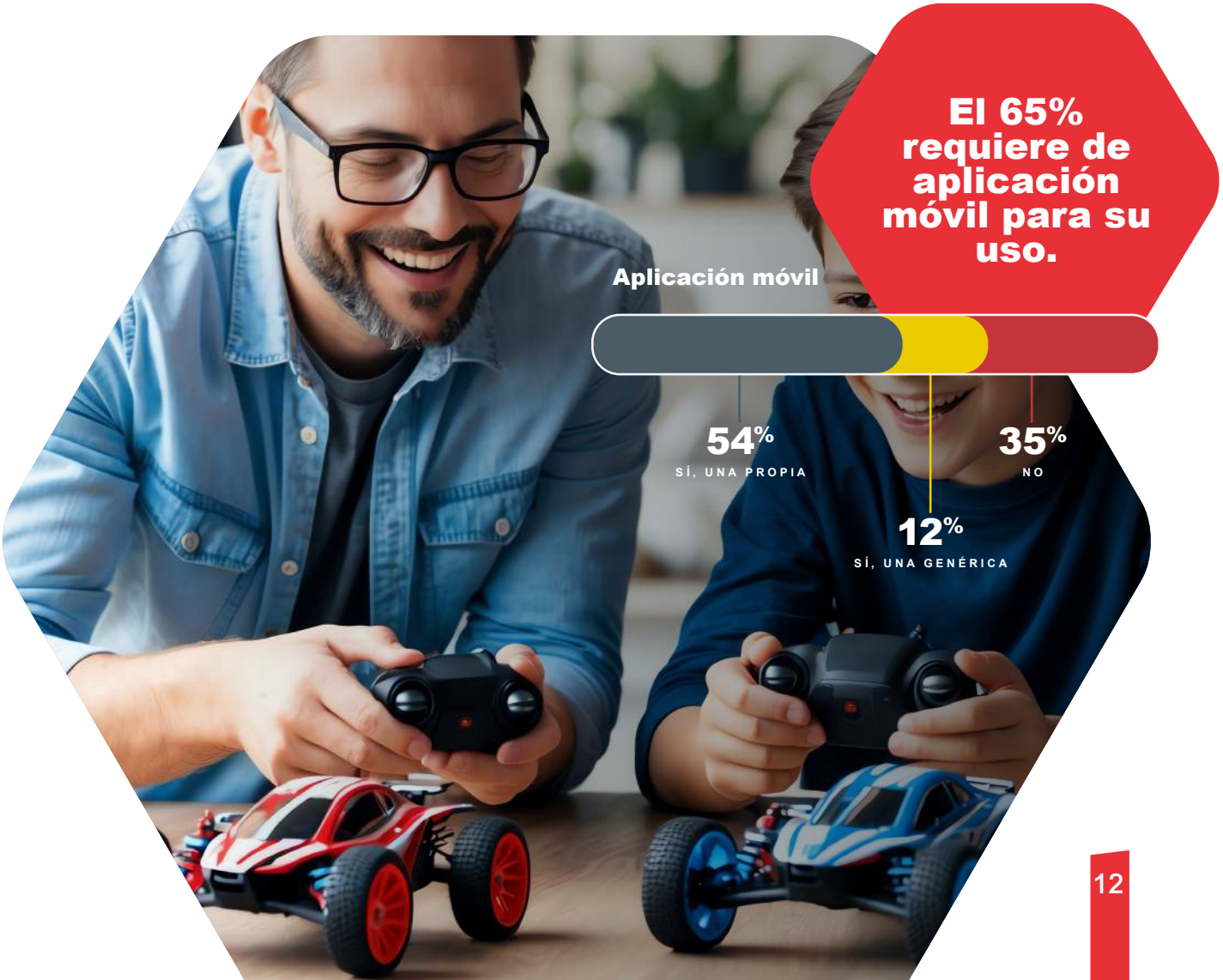
Pueden ser más robustas en términos de seguridad si están desarrolladas por empresas especializadas.

Una vulnerabilidad descubierta podría afectar a muchos productos conectados a la aplicación.

OPERABILIDAD Y CONFIGURACIÓN MANUAL:

Elimina la superficie de ataque relacionada con el ecosistema móvil.

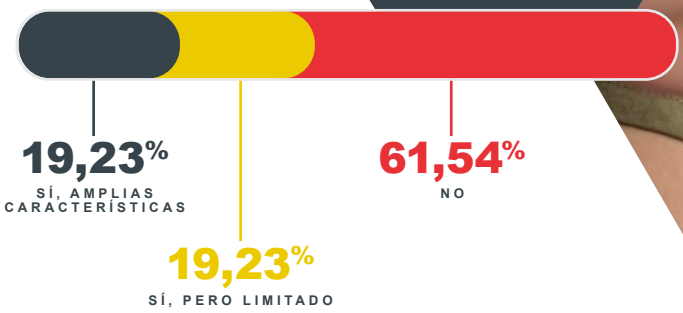
Dependencia de configuraciones manuales, que pueden ser más vulnerables a errores.



ESTADÍSTICAS **GENERALES**

Apenas el 40% hace uso del control parental.

Control parental



19,23%
SÍ, AMPLIAS CARACTERÍSTICAS

19,23%
SÍ, PERO LIMITADO

61,54%
NO

PREDOMINIO DE DISPOSITIVOS SIN CONTROL PARENTAL

Carecen de mecanismos básicos para protegerlos de contenido inapropiado o uso indebido.

Los padres dependen exclusivamente de supervisión manual o herramientas externas.

¿SEGURIDAD ROBUSTA IMPLICA SOBRE CONTROL?

Incrementan la confianza del usuario en el producto.

Pueden recopilar una gran cantidad de datos sensibles relacionados con los menores y sus actividades.

¿CONTROL LIMITADO IMPLICA FALSA SENSACIÓN DE SEGURIDAD?

Útil para escenarios sencillos, pero insuficiente frente a amenazas más complejas.

RESUMEN DE PUNTOS FUERTES
EN JUGUETES EVALUADOS

SEGURIDAD EN LA TRANSMISIÓN Y ALMACENAMIENTO DE DATOS

Uso de protocolos seguros como HTTPS y cifrado de extremo a extremo para proteger datos sensibles. Configuraciones iniciales que requieren contraseñas seguras y personalizadas. Almacenamiento local protegido mediante encriptación, evitando accesos no autorizados a información interna

PROTOCOLOS DE COMUNICACIÓN PROPIETARIOS

Dificultan la interceptación y manipulación de datos transmitidos, mejorando la privacidad.

DISEÑO SEGURO DE DISPOSITIVOS SIMPLES

Productos con menor conectividad y funcionalidades limitadas tienden a ser más seguros, al reducir la superficie de ataque.

REDES WI-FI SEGURAS

Las contraseñas robustas y la implementación de redes privadas ofrecen un acceso seguro al dispositivo.

TRANSPARENCIA Y COMPROMISO CON EL USUARIO

Productos que incluyen términos claros sobre el tratamiento de datos y notificaciones visibles en caso de cambios en políticas de privacidad. Comunicación directa al usuario sobre qué datos se recopilan, cómo se usan y la opción de deshabilitar funciones específicas para proteger su privacidad.

CERTIFICACIONES DE SEGURIDAD

Productos orientados a menores con certificaciones *"safe for children"* garantizan estándares básicos de ciberseguridad.

RESUMEN DE PROBLEMAS Y DEBILIDADES EN JUGUETES EVALUADOS

1 TRANSMISIÓN INSEGURA DE DATOS

Contraseñas, usuarios y otra información sensible viajan en texto claro por la **red local e Internet**, exponiéndose a interceptaciones.

2 PROBLEMAS DE AUTENTICACIÓN Y CONTROL

Permisos de administración accesibles a **usuarios no autorizados**. Posibilidad de control remoto del dispositivo por parte de atacantes a través de configuraciones deficientes.

3 APLICACIONES MÓVILES VULNERABLES

Almacenamiento inseguro de credenciales y datos personales. Presencia de **anuncios y "trackers"** que comprometen la privacidad del usuario.

4 CONFIGURACIONES INSEGURAS

Servicios y puertos innecesarios permanecen habilitados, ampliando la superficie de ataque. **Redes abiertas** (por ejemplo, Wi-Fi WEP o sin cifrado) facilitan la denegación de servicio o el secuestro de sesiones legítimas.

5 APLICACIONES MÓVILES VULNERABLES

Documentación técnica insuficiente y confusa. Escasez de soporte para incidentes o información pública clara sobre **vulnerabilidades** reportadas. Falta de alineación con regulaciones como el RGPD (tratamiento de datos personales) o la **Ley de Ciberresiliencia**, lo que pone en riesgo la confianza del usuario y expone a sanciones legales. Limitada información pública sobre el **tratamiento de datos**, como políticas de privacidad o procedimientos claros para solicitar la eliminación de datos personales.

6 GESTIÓN DEL *FIRMWARE* Y COMPONENTES OBSOLETOS

El ***firmware*** es accesible sin protección adecuada, muchas veces disponible públicamente o transferido sin cifrado durante las actualizaciones. Uso de bibliotecas, frameworks y sistemas operativos sin soporte, lo que incrementa las vulnerabilidades.

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD