Ciberseguridad en Smart Toys

Protección de menores y su entorno desde la fabricación

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

Asociación Española de Fabricantes de Juguetes

ÍNDICE

ÍNDICE

1 INTRODUCCIÓN

La Comisión Europea publicó el pasado 28 de enero de 2019 una iniciativa **[Ref - 1]** con la que se pretende regular la ciberseguridad de los dispositivos conectados a internet (IoT o Internet de las cosas, del inglés ***Internet of Things***) y equipos de radio portátil (wifi, NFC[1] , ***bluetooth***[2] ,...), entre ellos los juguetes con capacidad para conectarse a otros dispositivos, como teléfonos inteligentes, ordenadores o servicios en la nube.

Los juguetes tienen cada vez más capacidad para conectarse tanto a otros dispositivos como a diferentes servicios de Internet, lo que abre un nuevo escenario para que ciberdelincuentes y diferentes compañías, como las que realizan tratamientos masivos de datos personales, creación de perfiles o incorporan inteligencia artificial, puedan utilizar la información obtenida en su propio beneficio vulnerando los derechos de los consumidores. Además, estas interacciones de terceros pueden tener consecuencias para la privacidad y seguridad tanto del menor como de su entorno familiar.

Un estudio realizado en diciembre de 2016 **[Ref - 2]** por el *Norwegian Consumer Council*, referencia utilizada por la iniciativa europea citada anteriormente, analizó la privacidad y seguridad de varios juguetes conectados. Los resultados mostraron que los juguetes con capacidades de conexión a otros dispositivos carecían de las medidas de seguridad necesarias para proteger a un colectivo especialmente vulnerable, como son los menores.

Dado los crecientes riesgos relacionados con la ciberseguridad y el aumento de productos conectados, los Estados miembros de la UE han destacado que sería beneficioso aplicar un nivel mínimo de seguridad. Para ello, esperan que los fabricantes de productos conectados, como los juguetes, minimicen la recopilación de datos, realicen evaluaciones de privacidad, implementen estándares de privacidad y seguridad o los certifiquen, como garantías de seguridad adicionales a las del producto tradicional. El objetivo general de la iniciativa es garantizar un nivel adecuado de seguridad para los equipos comúnmente conocidos como *Smart Toys*.

En este contexto, esta guía recoge las medidas de protección que debe incorporar el fabricante durante todo el ciclo de vida del juguete, desde su fabricación hasta el momento en que deja de prestar soporte. También se incorporan las medidas

1. Near Field Communications, tecnología de comunicación inalámbrica de corto alcance y alta frecuencia.

2. Bluetooth es una especificación industrial para redes inalámbricas de área personal mediante un enlace de radiofrecuencia en la banda de 2,4 MHz

1

de seguridad que debe contar el juguete para su uso y configuración por padres y educadores a cargo de menores que utilicen estos dispositivos.

Por último recordar que los padres y educadores han de tener precaución y analizar las características de los dispositivos que se ponen al alcance de los menores antes de adquirirlos. En su uso, en ningún caso deben proporcionar al juguete datos que puedan servir para localizar al menor, y antes de compartirlos con terceros o desecharlos, han de tomar precauciones para borrar todos los datos que pudieran haber almacenado

2 VULNERABILIDADES Y RIESGOS EN SMART-TOYS

"Estos juguetes, generalmente, incorporan **funcionalidades multimedia** que les confieren simular tener una personalidad propia que interactúa con el menor"

Los fabricantes de juguetes están lanzando al mercado dispositivos para menores que incorporan conectividad a Internet y funcionalidades de inteligencia artificial. Llamamos **juguetes conectados** a aquellos que tienen la capacidad de comunicarse con otros dispositivos o a diferentes servicios de Internet que ofrecen una experiencia personalizada a los niños o a sus padres, al incorporar *software* de reconocimiento de voz y funcionalidad de búsqueda en la web. Los juguetes que ofrecen funcionalidades accesorias, a través de un portal web, como comunidades de usuarios, clubs de propietarios, etc., también son juguetes conectados

Por otra parte, también aparecen en el mercado **juguetes inteligentes** cuya electrónica y *software* les permiten aprender y modificar su comportamiento de acuerdo el entorno. Estos juguetes, generalmente, incorporan funcionalidades multimedia que les confieren simular tener una personalidad propia que interactúa con el menor. Tanto unos, como otros pueden tener funciones lúdicas y educativas cuya ética e idoneidad quedan fuera del ámbito de esta guía.

Como todo dispositivo electrónico con conectividad, los juguetes conectados y los juguetes inteligentes no están exentos de vulnerabilidades y riesgos de seguridad. Las primeras, las vulnerabilidades, pueden ser inherentes al diseño *hardware* y *software*, a su despliegue, a su configuración o a su uso. Los segundos, los riesgos, son la consecuencia de que en su utilización pueda llevarse a cabo un ciberataque contra la seguridad o la privacidad del usuario, aprovechando alguna de sus posibles vulnerabilidades.

2

Algunos de estos riesgos pueden provocar:

- pérdida de datos personales, en particular credenciales de acceso, datos almacenados, datos de uso, imágenes y sonido o datos de comunicaciones, con los consecuentes daños contra la privacidad de los menores;
- perfilado de usuarios con datos de uso y otras mediciones;
- toma de control remoto del dispositivo;
- interceptación de las comunicaciones o suplantación de alguno de los intervinientes.

Como se detalla en los apartados siguientes, los fabricantes incorporarán en sus procesos de producción **medidas organizativas y otras de carácter técnico** que favorezcan que el producto sea seguro para el usuario durante todo su ciclo de vida. Igualmente, las empresas que proporcionan y explotan las **aplicaciones web o apps para móviles** que se comunican con estos dispositivos, tendrán que incorporar medidas de seguridad.

La privacidad de los datos de los menores se puede ver seriamente comprometida por los juguetes dotados de capacidades de comunicación con otros dispositivos para compartir datos como la ubicación o conversaciones. Como se indica en los apartados siguientes se recomienda incorporar la privacidad desde el diseño **[Ref. - 3]** y por defecto **[Ref. - 4]**, por ejemplo, con mecanismos y controles, que favorezcan la minimización de la toma de datos personales, la autenticación, el cifrado de las comunicaciones o la obligación de cambiar las contraseñas por defecto, entre otros.

Los fabricantes también deben **incorporar información para padres y educadores** enfocada a evitar y descubrir malos usos, en particular cambios en la configuración de la privacidad, que puedan poner en riesgo la privacidad de los menores.

3 MEDIDAS DE SEGURIDAD EN LA FABRICACIÓN

El fabricante debe tomar las medidas organizativas y técnicas necesarias para mantener un adecuado nivel de privacidad y seguridad durante la fabricación y durante todo el ciclo de vida del producto, incluyendo el tratamiento de la información que se genere debido a su uso. A continuación, se incluyen algunas recomendaciones.

3.1. Establecer planes y roles de ciberseguridad

El fabricante debe contar con un Plan Director de Seguridad **[Ref. - 5]** en el cual estén identificados los procedimientos que recojan las medidas de seguridad que deben incorporarse enación y durante todo el ciclo de vida del juguete.

- La gestión de riesgos de ciberseguridad debe preceder al Plan Director de Seguridad, abarcando no solo la seguridad de los procesos de la empresa (fabricación, recursos humanos, servicios TIC, etc.), sino también en el propio juguete fabricado, incorporando ensayos de ciberseguridad, tales como auditorías de todos los componentes tecnológicos que lo conforman.
- Para el análisis de riesgos **[Ref. - 6]** en los tratamientos de datos personales que afecten a los usuarios de los juguetes se ha de seguir la Guía práctica **[Ref. - 7]** de la AEPD **[Ref. - 8]** (Agencia Española de Protección de Datos)
- Se deben establecer distintos roles y responsabilidades **[Ref. - 9]**, —entre otros los responsables de seguridad

3

de la información o CISO[3] y de privacidad o DPO[4] — de los profesionales encargados de garantizar la ciberseguridad y la privacidad de los juguetes fabricados.

» En particular, para el cumplimiento de la legislación en materia de protección de datos, se han de identificar los responsables del tratamiento de datos personales y el DPO o Delegado de Protección de Datos **[Ref. - 10]**.

3.2. Formación de los empleados

Los empleados son un eslabón imprescindible para incorporar seguridad en todo el ciclo de vida del juguete. Para garantizar el correcto tratamiento los planes de seguridad deben incluir también planes de formación y concienciación. .

» Se promoverán entre el personal de la organización el conocimiento y la aplicación de prácticas que mejoren la privacidad y seguridad de la información en la empresa y en los productos que se fabrican.

» Se recomienda implantar medidas de concienciación para todo el personal que pueden incluir los recursos ofrecidos desde INCIBE, entre otros:

→ Charlas de concienciación **[Ref. - 11]**
→ Itinerarios interactivos para el sector industrial **[Ref. - 12]**
→ Desarrollar cultura en seguridad **[Ref. - 13]**

» Se recomienda implantar un plan de formación **[Ref. - 14]** que aumente los conocimientos de ciberseguridad de los empleados, especialmente entre aquellos involucrados en el desarrollo y la fabricación del juguete o en el tratamiento posterior de los datos generados por los usuarios. Se hará especial hincapié en los aspectos relativos a la privacidad y protección de los menores.

3.3. Certificaciones y seguridad desde el diseño y por defecto

En la fabricación del producto se han de tomar medidas encaminadas a incorporar garantías de seguridad y privacidad en el producto terminado:

» Se recomienda promover el uso de tecnologías y soluciones estandarizadas libres, evitando el uso de soluciones propietarias. Al estar las soluciones libres

3 Chief Information Security Officer o responsable de seguridad de la información, generalmente en el ámbito de la ISO 27001

4 Data Privacy Officer o Delegado de protección de datos (DPD) es la figura de asesor de privacidad en el ámbito del RGPD, el Reglamento General de Protección de Datos.

soportadas por una comunidad amplia, se espera que su seguridad esté más controlada y reciban más rápido actualizaciones en caso de que presenten vulnerabilidades.

- En el juguete se deben incorporar desde el diseño **[Ref. - 3]** y por defecto **[Ref. - 4]** las medidas adecuadas para garantizar la protección de la privacidad y seguridad del menor.
- Uso de tecnologías con certificaciones de seguridad **[Ref. - 15]** o la certificación de los productos terminados que permitirá aportar garantías al juguete.

3.4. Gestión de las vulnerabilidades descubiertas

Internamente, una buena gestión de las vulnerabilidades de los productos va a favorecer la corrección de las mismas en el mínimo tiempo posible, minimizando así los riesgos para los usuarios.

- Se deben implantar mecanismos para promover las investigaciones en ciberseguridad y que faciliten el reporte de las vulnerabilidades descubiertas, como un punto de contacto único para el reporte o programas que incentivan el descubrimiento (*Bug Bounty* **[Ref. - 16]**) por investigadores y terceros.
- Se debe crear una política empresarial para comunicar e informar de aquellas vulnerabilidades entre los diferentes actores involucrados con el producto, como desarrolladores, fabricantes, proveedores y equipos de respuesta a incidentes.
- Se establecerán procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

3.5. Garantías durante y al final del ciclo de vida del producto

El usuario tiene a su disposición las garantías necesarias durante y al final del ciclo de vida de un producto:

- Se informará al usuario del uso correcto del producto, para evitar poner en riesgo la privacidad o la seguridad de los menores.
- Se garantizará que el producto se actualice de forma automática por defecto para aplicar los parches de seguridad de las vulnerabilidades conocidas hasta la fecha de fin de soporte.
- Se informará al consumidor de la fecha en que se producirá el final de soporte para el producto, momento en que el fabricante puede optar por dejar de liberar parches de seguridad. Se informará a los consumidores de los riesgos que pueden correr si continúan utilizando el dispositivo una vez

3

finalizado el periodo de soporte. Por ejemplo: «*A partir del día XX de XXXXX de XXXX finalizará el soporte técnico del dispositivo XXXXXXXXXXXXX, después de dicha fecha, las actualizaciones que ayudan a proteger el dispositivo dejarán de estar disponibles*.» **Este mensaje depende del ciclo de vida del producto, por lo que debe redactarse por el equipo jurídico de la empresa**.

4 SEGURIDAD INCORPORADA EN EL JUGUETE

"Estos dispositivos requieren, generalmente, iniciar sesión con **mecanismos de autenticación.** El más frecuente es la utilización de usuario y contraseña."

Cuando se habla de juguetes conectados se hace referencia a aquellos que incorporan las prestaciones necesarias o accesorias para su funcionamiento, a través de internet o que permiten la interacción con otros dispositivos como tabletas, *smartphones* o *smartwatches*, mediante tecnologías muy diversas como *wifi* o *bluetooth*. Esto también es cierto, en la mayoría de los casos, para juguetes inteligentes.

Para maximizar las garantías de seguridad de estos dispositivos, de la información que gestionan, los sensores y permisos a los que tienen acceso el fabricante o integrador, tiene que aplicar una serie de medidas.

4.1 Mecanismos de autenticación seguros

Estos dispositivos requieren, generalmente, iniciar sesión con mecanismos de autenticación. El más frecuente es la utilización de usuario y contraseña. Se han de forzar en el diseño del interfaz estas medidas para evitar que sea vulnerado el acceso.

- Se protegerán los inicios de sesión contra ataques de fuerza **[Ref. - 6]** bruta bloqueándolos o deshabilitándolos temporalmente después de un número razonable de intentos de sesión no válidos
- El mecanismo habilitado en caso de olvido de la contraseña de acceso no proporcionará a los atacantes información que pueda ser utilizada en posteriores ataques, como por ejemplo cuentas de usuario validadas.

4

- La contraseña y el nombre de usuario o código de acceso por defecto con las que cuente el dispositivo, deben ser modificados en el primer inicio de sesión que se realice. La nueva contraseña debe ser robusta y no se permitirá utilizar una que no lo sea.
- En caso de que el dispositivo cuente con una contraseña y usuario de fábrica, bien serán específicas (nunca universales como «admin», «admin» o similares) para cada dispositivo concreto, o bien se forzará el cambio de esta en el primer uso. Idealmente, cada dispositivo tendrá una identidad única.
- El dispositivo no deberá tener ningún tipo de usuario y contraseña embebidas en el código del dispositivo/aplicación.
- Ofrecer la posibilidad de utilizar mecanismos de doble factor de autenticación para evitar accesos no autorizados al dispositivo.

4.2 Cifrado de la información

La información en el dispositivo o la que circula en sus comunicaciones con otros dispositivos o a través de internet, tiene que estar protegida ante posibles ataques contra su confidencialidad e integridad, como los producidos en caso de interceptación de las comunicaciones. El cifrado de esta información es básico para este propósito.

- Se utilizarán algoritmos de cifrado **[Ref. - 6]** seguros y conocidos por la comunidad, es decir que no hayan sido comprometidos, para mantener la confidencialidad, autenticidad e integridad de la información, tanto almacenada en el propio dispositivo, como el tránsito hacia otros dispositivos o servicios.
- Las claves criptográficas deben ser gestionadas de forma segura, ya que en caso de que estas se comprometan, el cifrado y por lo tanto, la información también lo estarían.

4.3 Actualizaciones de seguridad

En caso de existir vulnerabilidades, se han de tomar las siguientes medidas para reducir el riesgo al que están expuestos los usuarios.

- Se han de actualizar, de forma segura, todos los componentes que integran el juguete.
- En caso de ser necesaria una actualización de seguridad, el fabricante o el proveedor del servicio, deben comunicarse con el usuario para indicarle que ha de actualizarlo. La actualización se realizará lo antes posible y será fácil de implementar por el usuario.

4

- El fabricante o el desarrollador de componentes actualizables publicarán, de forma accesible y transparente para el usuario, una política con el tiempo mínimo durante el cual recibirá actualizaciones. Los componentes no actualizables, se podrán aislar de la red y ser reemplazados con la ayuda de la asistencia técnica. Una política transparente y accesible indicará el periodo de soporte de estos componentes.
- Se han de ofrecer mecanismos automáticos y seguros de actualización, preferiblemente, vía OTA (*Over-The-Air*). Este tipo de actualización permite la descarga e instalación del nuevo *software* sin necesidad de tener que conectarlo a otro dispositivo, ya que se realiza por medio de tecnologías inalámbricas como *wi i*. El servidor utilizado para enviar la actualización será seguro, los datos estarán cifrados y firmados manteniendo así la confidencialidad e integridad de la actualización.
- El *software* del dispositivo se verificará utilizando mecanismos de arranque seguros que requieran una raíz de confianza basada en *hardware* para evitar que se instale en el arranque *software* no autorizado (*rootkits*). En caso de que el dispositivo detecte un cambio no autorizado del *software*, debe alertar al usuario y al administrador, no conectarse a redes salvo para realizar esta alerta.
- La actualización automática del dispositivo debe ser una opción que se encuentre por defecto habilitada.
- Las actualizaciones de seguridad no deben modificar ninguna configuración que haya realizado el usuario.

4.4 Otras cuestiones de seguridad

Además, se han de observar configuraciones por defecto que ofrezcan garantías de seguridad.

- Se habilitarán por defecto todas las características que mejoren la seguridad en el dispositivo.
- Una vez se ha pasado el dispositivo a la fase de producción se deshabilitará cualquier servicio que no sea necesario para el correcto funcionamiento del mismo. Se eliminará el *software* y se cerraran puertos de red no utilizados. Se deshabilitarán puertos o puntos de chequeo que se hubieran habilitado en fase de desarrollo. Se minimizará el código, de manera que sea solo el imprescindible para el funcionamiento del dispositivo.
- Se ejecutará el *software* con los mínimos privilegios necesarios considerando funcionalidad y seguridad.

4

"En caso de fallos de red o de alimentación, el dispositivo tendrá un modo de **funcionamiento local** que permitirá su reconexión cuando se restauren los servicios"

- Se habilitará un sistema que permita restaurar el dispositivo a los valores por defecto de fábrica.
- Cuando un nuevo dispositivo se vincule con el juguete este emitirá una señal sonora y visual.
- El juguete en el momento de su venta o distribución debería estar actualizado a la última versión, en caso de no ser posible, notificará al usuario de la disponibilidad de una nueva versión.
- En caso de fallos de red o de alimentación, el dispositivo tendrá un modo de funcionamiento local que permitirá su reconexión cuando se restauren los servicios.
- La instalación y mantenimiento del dispositivo será sencilla, con el mínimo de pasos posibles y tendrá en cuenta las mejores prácticas de seguridad y usabilidad. En caso de ser necesario, se proporcionará un manual para el arranque inicial seguro del dispositivo.

5 CÓMO GARANTIZAR LA PRIVACIDAD

Siempre que el juguete o los dispositivos relacionados con su uso tengan acceso a datos personales del menor, la empresa o empresas que traten estos datos, en particular las que despliegan y explotan las apps y las aplicaciones web, han seguir las siguientes recomendaciones para cumplir con la ley.

5.1 Aspectos específicos del tratamiento de datos de menores

Llevar a cabo un correcto tratamiento de los datos, especialmente cuando se trata de menores, es imprescindible para garantizar su privacidad y seguridad. Así el "*Artículo 38*" del Reglamento General de Protección de Datos **[Ref. - 17]:**

» «Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños.»

En primer lugar el tratamiento estará fundado en el **consentimiento**, que será obtenido de forma válida e inequívoca y será **lícito** si se cumple el artículo 7 sobre el Consentimiento de los menores de edad de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos

5

"El tratamiento de los datos personales de un menor de edad, únicamente podrá fundarse en su consentimiento **cuando sea mayor de catorce años**"

Digitales **[Ref. - 18]** LOPDGDD:

- «El tratamiento de los datos personales de un menor de edad, únicamente podrá fundarse en su consentimiento **cuando sea mayor de catorce años**. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.»
- «El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.»

Y también se ha de contemplar en cuanto al **ejercicio de los derechos** lo indicado en el artículo 12 Disposiciones generales sobre el ejercicio de los derechos:

- «[..] los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años, los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.»

Además en lo relativo a la **información al interesado** (el menor o los titulares de la patria potestad) sobre el tratamiento y sus derechos, también debe ser conforme al Reglamento General de Protección de Datos **[Ref. - 17]** que en su artículo 12.1 indica que debe «ser concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño.» Se proporcionará información sobre cómo se utilizarán sus datos personales, por quién y para qué, para cada dispositivo o servicio, incluyendo el uso que hagan terceros de estos datos.

5.2 Relaciones con terceros

En cuanto a las relaciones del fabricante con terceros:

- Se compartirán, únicamente, datos personales con terceras partes cuando se cuente con el consentimiento

de los usuarios, además las terceras partes deben cumplir con las mismas o más restrictivas políticas de privacidad y seguridad que el fabricante.

- Si en el tratamiento de los datos personales de usuarios de juguetes intervinieran terceros, también se ha de seguir las directrices para la elaboración de contratos entre responsables y encargados del tratamiento **[Ref. - 19]** de la AEPD, la Agencia Española de Protección de Datos.
- Los fabricantes de *hardware* y de *software* deben adoptar medidas para la prevención de riesgos de ciberseguridad en su cadena de suministro, ya que podrían ser objeto de este tipo de ataques en los que el ciberdelincuente se infiltra en el sistema a través de un proveedor o socio externo. De esta forma, pueden incorporar *malware* **[Ref. - 6]** o *hardware* falsificado en los componentes de los proveedores que podrían afectar al producto una vez adquirido el usuario. Estas modificaciones podrían derivar en riesgos para la seguridad y privacidad de los menores que es necesario identificar. Por ello el fabricante debe:
  - → comprobar la seguridad de sus proveedores y desarrolladores de *software*;
  - → implementar directivas de integridad de código;
  - → utilizar soluciones de detección y respuesta.

5.3 Disposiciones generales de la LOPDGDD

También se han de tener en cuenta otras disposiciones generales de la Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales.

5.3.1. ¿Cómo cumplir la ley?

Para cumplir con la LOPDGDD también se deben garantizar los derechos y libertades de las personas en cuanto a sus datos personales. Para ello:

- Se han de identificar si se hacen tratamientos de alto riesgo, con datos especialmente protegidos o a gran escala. Los datos especialmente protegidos son aquellos cuyo tratamiento pudiera entrañar importantes riesgos para los derechos y las libertades fundamentales. Estos datos son los relativos a origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, salud, vida y orientación sexual y los datos genéticos y biométricos. Si se considera que no se realizan tratamientos de alto riesgo, se debe justificar la decisión.
- Se han de garantizar los derechos y libertades de los individuos con respecto a sus datos personales:
  - → informándoles **[Ref. - 20]** de forma visible, accesible, sencilla y

5

"Se han de garantizar los **derechos y libertades de los individuos** con respecto a sus datos personales"

"Se han de revisar los contratos con los encargados de **tratamiento de información**, si se contratan servicios externos que utilicen los datos personales de los tratamientos"

transparente sobre el tratamiento de sus datos;
→ obteniendo de ellos el consentimiento inequívoco o expreso según las categorías de datos del tratamiento;
→ permitiéndoles ejercitar sus derechos **[Ref. - 21]** de forma sencilla, trasparente, y en los plazos previstos;
→ notificándoles en caso de violaciones de seguridad que pudieran afectarles.

» En general se ha de realizar una evaluación de riesgos para establecer las medidas técnicas y organizativas necesarias para garantizar el nivel de seguridad adecuado al riesgo existente.

» Se han de revisar los contratos con los encargados **[Ref. - 19]** de tratamiento de información, si se contratan servicios externos que utilicen los datos personales de los tratamientos. Se debe limitar al máximo posible el acceso de terceras partes a los datos personales de los clientes.

» Se ha de establecer un proceso de verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas que se hayan aplicado.

5.3.2. Tratamientos de alto riesgo

Se ha de tener en cuenta lo siguiente si tras realizar una evaluación de riesgos se determina que el tratamiento de datos es de alto riesgo.

» Se ha de llevar un registro de actividad si el tratamiento es de alto riesgo o si se realiza de forma no ocasional, pudiendo entrañar riesgos para la privacidad o con categorías especiales de datos.

» Además la empresa deberá tener un DPD o Delegado de protección de datos **[Ref. - 22]** y realizar un Análisis de impacto del tratamiento **[Ref.**

- 23] en particular cuando se lleve a cabo el (Art. 28 2 e. LOPDGDD) «tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad».

5.3.3. Todo tipo de tratamientos

En cualquier tipo de tratamiento de datos personales se han de tomar algunas medidas organizativas y de adecuación de protocolos internos.

- Se deben adecuar los procedimientos y canales para informar, recabar el consentimiento, permitir el ejercicio de los derechos y notificar en caso de brecha de seguridad que afecte a la privacidad de los usuarios.
- Se han de implantar políticas **[Ref. - 24]** para garantizar la seguridad de los tratamientos.
- Es necesario formar y concienciar a todos los empleados que intervengan en los tratamientos. Utiliza los recursos de formación **[Ref. - 25]** y el kit de concienciación.

5.3.4. Medidas técnicas a implantar

Con el objetivo de controlar los datos personales en todo momento, garantizar los derechos a los usuarios y además poder demostrarlo, tanto el fabricante como el resto de empresas que hagan uso de los datos personales recopilados han de utilizar herramientas tecnológicas que permitan:

- Determinar dónde están ubicados los datos, clasificarlos según su criticidad, monitorizar su uso, conocer quién accede, cuando se borran y cifrarlos cuando sea necesario.
- Evitar accesos no autorizados y restringir el acceso a los datos aplicando principios de mínimos privilegios mediante sistemas de gestión de identidad y autenticación.
- El cifrado garantiza la confidencialidad y la integridad, reduce el riesgo de sanciones y evita tener que informar a los usuarios en caso de brecha de seguridad.
- Realizar *backups* (copias de seguridad) mediante instrumentos específicos de contingencia y continuidad.

En el dispositivo y en las aplicaciones web o app en móviles:

- Si el dispositivo o sus aplicaciones recogen datos de uso o de otro tipo de mediciones, se examinarán para detectar anomalías de seguridad,

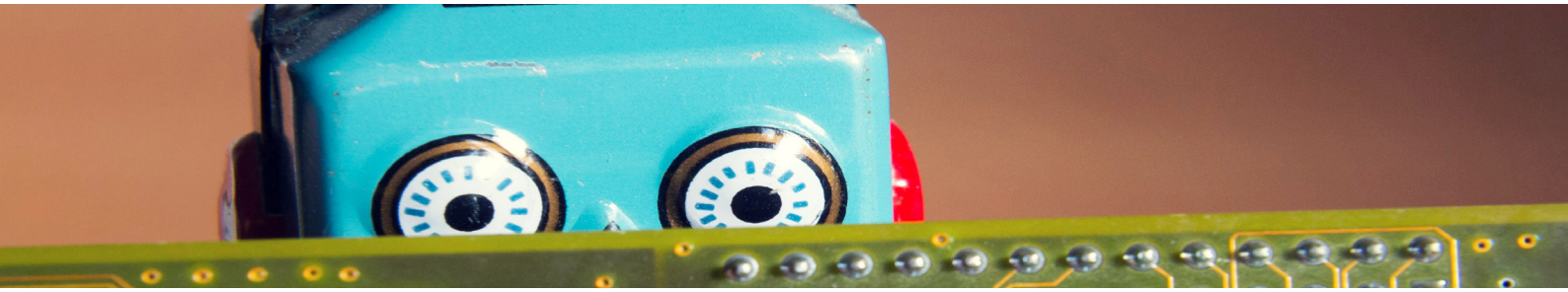
se minimizará la recogida de datos personales y se anonimizarán, y se avisará a los usuarios de los datos recogidos y los propósitos

- Se habilitarán mecanismos sencillos e instrucciones claras para que los usuarios borren sus datos personales en caso de cambios de titularidad o si quiere borrarlos por otro motivo (incluidas copias de seguridad) o para deshacerse del dispositivo. Una vez borrados los datos el usuario, este recibirá una confirmación inequívoca de que han sido borrados de todas las aplicaciones y servicios, y del dispositivo.

5.3.5. Informar a los usuarios de su responsabilidad

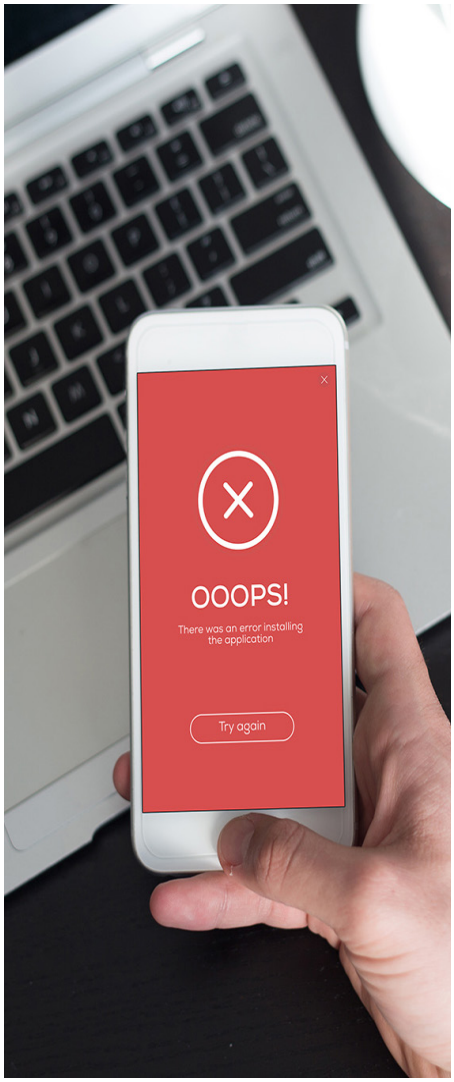
Según el Art. 84 de la LOPDGDD (Protección de los menores en Internet) también los padres y otros representantes de los menores tienen que procurar que estos hagan un uso correcto de los servicios y dispositivos. Por ello, debemos recordar el contenido de este artículo:

- «Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.»
- «La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.»



6 SEGURIDAD DE LA APLICACIÓN MÓVIL

En los casos en que el juguete tenga asociada una aplicación móvil para su uso o como complemento de este se deben seguir una serie de recomendaciones de seguridad para proteger la privacidad y seguridad del menor.



6.1 Almacenamiento de datos y privacidad

En el diseño de la aplicación y en sus opciones por defecto:

- Se utilizará la función de almacenamiento de credenciales del sistema operativo del dispositivo móvil para guardar usuarios, contraseñas y claves criptográficas.
- Se comprobará que los registros de actividad (*logs*) generados por la aplicación no filtran ningún tipo de información sensible.
- Se compartirá la mínima información personal posible con terceros.
- Se desactivará la caché del teclado y la función de portapapeles en los campos de texto donde se maneja información sensible
- No se expone información sensible mediante mecanismos IPC (comunicación entre procesos del sistema operativo, del inglés *Inter-Process Communication*, para compartir espacios de memoria, variables, sincronizarse, etc., según protocolos establecidos).

6.2 Cifrado

Siempre que se traten datos de carácter personal o confidencial:

- Se deben utilizar tanto métodos criptográficos simétricos

como de clave pública **[Ref. - 6]**.

- La aplicación utilizará métodos criptográficos probados y robustos, evitando soluciones propietarias.
- Los valores aleatorios son generados mediante un mecanismo lo suficientemente robusto como para que no puedan ser predichos.
- Se indicará al usuario que no debe utilizar la misma clave para varios propósitos, ya que si se utiliza la misma en varios servicios y en uno de ellos se ve comprometida, lo estará en el resto de servicios que utilicen la misma.

6.3 Autenticación y manejo de sesiones

Las aplicaciones requieren que el usuario se autentique iniciando una sesión cada vez que esto ocurre. Existen distintas formas de gestionar estas sesiones y se han de contemplar las distintas situaciones y verificar que se cumple lo siguiente:

- Si la aplicación utiliza un servicio remoto que requiera credenciales de acceso como usuario y contraseña, estas serán validadas en el lado del servidor.
- Si se utilizan estados para la gestión de sesiones, el servidor remoto utilizará *tokens* o identificadores de acceso aleatorios para autenticar las solicitudes del cliente, sin requerir el envío de las credenciales del usuario en cada uno de ellos.
- Si se utiliza la autenticación basada en *tokens* sin estado, el servidor proporcionará un *token* firmado utilizando un algoritmo seguro.
- Cuando el usuario cierra sesión en la aplicación también se cierra en el servidor.
- Existe protección contra ataques de fuerza bruta.
- Las sesiones y los *tokens* de acceso expiran después de un tiempo predefinido de inactividad.

6.4 Comunicación

Las aplicaciones se comunican con servidores para desplegar su funcionalidad o permiten la comunicación entre usuarios. En ambos casos se ha de tener en cuenta:

- La información, incluida la información de control y gestión, se envía cifrada utilizando las mejores prácticas posibles en su implementación, tanto con el juguete como con el servidor remoto.
- La aplicación verifica el certificado X.509[5] del servidor al establecer el canal

5 Estándar UIT-T (Sección de Normalización de la Unión Internacional de Telecomunicaciones) para

seguro y solo se aceptan certificados firmados por una CA (Autoridad de Certificación) válida.

6.5 Interacción con el sistema operativo

La aplicación también interactúa con el sistema operativo del dispositivo en el que se instala. Se han de seguir las siguientes pautas:

- La aplicación requerirá la mínima cantidad de permisos posible para su correcto funcionamiento.
- Toda entrada de información, tanto del usuario, como de fuentes externas debe ser validada y filtrada de forma que no contenga código malicioso.
- La aplicación no exporta datos sensibles, como identificadores de usuario, nombres o números de teléfono en las direcciones web utilizadas para comunicarse o que indexan los buscadores como Google, salvo que estén debidamente protegidos.
- Si la aplicación utiliza navegadores integrados o *WebViews* debe estar prohibido el uso del lenguaje de programación JavaScript (con la extensión .js) salvo que sea necesario. Preferiblemente se utilizarán aquellos que cuenten con protocolos de comunicación seguros como HTTPS.
- La serialización de objetos (proceso en el que un objeto se envía a través de una conexión en red en una serie de *bytes* o en un formato como XML o JSON, siendo el nuevo objeto idéntico al original) se implementa utilizando interfaces de programación de aplicaciones o API (*Application Programming Interfaces*) seguras.

6

"La aplicación tiene que estar firmada y provista con un **certificado válido**."

6.6. Calidad de código y configuración del compliador

En cuanto a los requisitos de seguridad del programa y la configuración del compilador que hace que este código sea inteligible para la máquina, se han de seguir los siguientes requisitos:

- La aplicación tiene que estar firmada y provista con un certificado válido.
- Se eliminará del código fuente cualquier mecanismo de depuración utilizado en su desarrollo.
- Todos los componentes de terceros se encuentran identificados y revisados por vulnerabilidades conocidas.
- La aplicación captura y maneja debidamente las posibles excepciones y errores que se pueden producir durante la ejecución de la misma y que si no son controlados debidamente pueden llegar ser explotados de forma maliciosa, como por ejemplo los desbordamientos de búfer **[Ref. - 6]** (*Buffer Overflow*).
- Antes de liberar la aplicación se realizarán pruebas de penetración para comprobar la seguridad de la misma frente a intrusiones, es decir personal con los suficientes conocimientos técnicos evaluara la seguridad de la aplicación.

7 SEGURIDAD DE LA APLICACIÓN WEB

En los casos en que el juguete tenga asociada una aplicación móvil para su uso o como complemento de este se deben seguir una serie de recomendaciones de seguridad para proteger la privacidad y seguridad del menor.

7.1. Autenticación

Estas aplicaciones web requieren, generalmente, iniciar sesión con mecanismos de autenticación. El más frecuente es el uso de usuario y contraseña. Se han de incorporar en el diseño del interfaz estas medidas para evitar que sea vulnerado el acceso.

- Habilitar mecanismos de protección, como el bloqueo de la cuenta, en caso de que se produzcan ataques de fuerza bruta (intentos de entrar con todas las combinaciones posibles) o repetidos intentos de sesión erróneos.
- Las contraseñas de inicio de sesión deben ser robustas, es decir, difíciles de descifrar, y no se permitirá utilizar contraseñas que no cumplan con los requisitos necesarios, como longitud, complejidad (uso de distintos tipos de caracteres, por ejemplo) y la prohibición de repetirla, entre otros.
- Cuando se quiera modificar la contraseña, el usuario debe proporcionar la antigua, una vez cambiada se le enviará una notificación como confirmación.
- Ante una contraseña olvidada esta debe cambiarse y nunca recuperarse. Las contraseñas no se almacenarán de forma que se permita su recuperación, para ello contarán con mecanismos de cifrado.
- Las credenciales de acceso de los usuarios y otros datos sensibles se almacenarán en los dispositivos o servicios

utilizando técnicas de cifrado robustas, es decir, difíciles de descifrar. Nunca se utilizarán credenciales predefinidas y fijas (*hard-coded*) en el dispositivo.

- Se utilizarán métodos de cifrado SSL (protocolo para asegurar las comunicaciones intercambiando claves de cifrado) en todas las páginas de inicio de sesión.
- El navegador almacena copias de las páginas en una memoria llamada caché para poder cargarlas más rápido si el usuario vuelve a solicitarlas. En las páginas de inicio de sesión no se debe permitir deshabilitar esta caché (utilizando etiquetas «no cache») para impedir que se hagan copias de la página de inicio de sesión, incluida la sesión, ya que un usuario malintencionado podría hacer una copia de esta y acceder al sistema sin tener permiso para ello.
- Emplear mecanismos de doble factor de autenticación para evitar accesos no autorizados y proteger la información.

7.2. Control de accesos

El acceso de usuarios a la aplicación web ha de estar gestionado de forma segura garantizando que:

- Los usuarios deben tener acceso únicamente a su perfil de usuario, no podrán acceder a áreas de otros usuarios o archivos del sistema.
- La actividad de los usuarios no se almacena en la memoria caché cuando se maneja información confidencial.
- Se realizarán pruebas de penetración antes de mover la aplicación a un entorno de producción y se comprobará que los usuarios únicamente tienen permiso de acceso a su perfil.

7.3. Gestión de sesiones

Las aplicaciones web requieren que el usuario se autentique iniciando una sesión cada vez que esto ocurre. Existen distintas formas de gestionar estas sesiones y se han de contemplar las distintas situaciones y verificar que se cumple lo siguiente:

- Las *cookies*, archivos almacenamos en el equipo del usuario que pueden servir, entre otros, para su identificación, no deben contener o utilizarse para obtener información confidencial del usuario.
- El usuario debe aceptar la política de cookies para poder utilizar la aplicación web.
- Los identificadores de sesión o *tokens* serán únicos para cada usuario y serán emitidos únicamente después de una autenticación exitosa, para ello se

7

"Los tokens deben estar protegidos para evitar que un usuario sin autorización pueda **secuestrarlos y suplantar la identidad** del usuario legítimo."

"[...] Estos datos **pueden ser alterados** para incluir código malicioso.[...]"

utilizará una fuente aleatoria de confianza.

» El identificador de sesión o *token* no contendrá información confidencial.

» Los *tokens* deben estar protegidos para evitar que un usuario sin autorización pueda secuestrarlos y suplantar la identidad del usuario legítimo.

» Los *tokens* tendrán un tiempo de vida limitado ante sesiones inactivas. Las sesiones activas también tendrán un tiempo de vida limitado antes de que se genere un nuevo *token*.

» Los *tokens* estarán protegidos mediante técnicas de cifrado robustas.

» Al cerrar sesión se debe sobrescribir el *token*.

7.4. Validación y filtrado de datos de entrada

Las aplicaciones web reciben datos, bien de formularios o bien a través de comunicaciones entre aplicaciones. Estos datos pueden ser alterados para incluir código malicioso. Para evitar este tipo de ataques:

» Se comprobará cualquier dato de entrada en la aplicación web siguiendo buenas prácticas en el validación y filtrado de datos de entrada.

» La validación y filtrado de los datos de entrada se realizará en el servidor, en el lado cliente se puede hacer una primera validación, pero no ha de ser la única.

7.5. Cifrado

La información que circula en las comunicaciones hacia y desde la aplicación web, tiene que estar protegida ante posibles ataques contra su confidencialidad e integridad, como los producidos en caso de interceptación de las comunicaciones.

7

El cifrado de esta información es básico para este propósito.

- Se implementarán técnicas de cifrado robustas de la información en toda la aplicación web.
- Se utilizarán técnicas de cifrado de dominio público y reconocidas por la comunidad, evitando el uso de métodos de cifrado propietarios.

7.6. Control de los mensajes de error

Los mensajes de error de la aplicación web pueden ser utilizados por los ciberdelincuentes para localizar páginas vulnerables

- Las páginas de error no deben mostrar información confidencial o que pueda ser utilizada para realizar ataques contra la aplicación.
- Se llevará un registro de los errores producidos.

7.7. Logs

Los registros de eventos de las aplicaciones web (*logs*) son ficheros de texto que registran la traza de todos los sucesos e interacciones entre los clientes (navegadores) y servidores web, como autenticaciones o peticiones de páginas. Estos tienen que contemplar los siguientes mecanismos de seguridad.

- Los sellos de tiempo de las entradas (cada uno de los eventos) en los logs deben ser precisos. Se deben sincronizar los sistemas con un servidor de tiempo fiable (vía protocolos específicos).
- Se llevará un registro lo más exhaustivo posible de todos los eventos que suceden en la aplicación, tanto de usuarios, como de administradores.
- Los *logs* también deben estar cifrados.

8 REFERENCIAS

[Ref - 1]. **European Commission - Internet-connected radio equipment and wearable radio equipment -** https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-6426936_en

[Ref - 2]. **Forbruker Rådet – Connected toys violate European consumer law -** https://www.pcisecuritystandards.org/document_ library?agreements=pcidss&association=pcidss

[Ref - 3]. **Enisa - Privacy and Data Protection by Design -** https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

[Ref - 4]. **Enisa - Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default -** https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2

[Ref - 5]. **INCIBE – Protege tu empresa – ¿Qué te interesa? – Plan director de seguridad -** https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad

[Ref - 6]. **INCIBE – Protege tu empresa – Guías - Glosario de términos de ciberseguridad: una guía de aproximación para el empresario -** https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario

[Ref - 7]. **Agencia española de protección de datos – Guía práctica de análisis de riesgos en los tratamientos de datos personales al RGPD -** https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

[Ref - 8]. **Agencia española de protección de datos -** https://www.aepd.es/

[Ref - 9]. **INCIBE – Protege tu empresa – Blog - CEO, CISO, CIO… ¿Roles en ciberseguridad? -** https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad

[Ref - 10]. **INCIBE – Protege tu empresa – Blog - DPD o DPO, el Delegado de la Privacidad -** https://www.incibe.es/protege-tu-empresa/blog/dpd-o-dpo-el-delegado-privacidad

[Ref - 11]. **INCIBE – Protege tu empresa - Talleres ciberseguridad para micropymes y autónomos -** https://www.incibe.es/protege-tu-empresa/talleres-ciberseguridad-pymes

[Ref - 12]. **Itinerarios interactivos – Sector industria -** https://itinerarios.incibe.es/?contador_pagina=2&IT_actual=1

8

[Ref - 13]. **INCIBE – Protege tu empresa - ¿Qué te interesa? – Desarrollar cultura en seguridad -** https://www.incibe.es/protege-tu-empresa/que-te-interesa/desarrollar-cultura-en-seguridad

[Ref - 14]. **INCIBE – Protege tu empresa - ¿Qué te interesa? - Protección de la información -** https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

[Ref - 15]. **European Commission - The EU cybersecurity certi ication framework -** https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

[Ref - 16]. **Wikipedia - Bug bounty program -** https://en.wikipedia.org/wiki/Bug_bounty_program

[Ref - 17]. **Diario Oficial de la Unión Europea - REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO -** https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=es

[Ref - 18]. **Boletín Oficial del Estado - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales -** https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

[Ref - 19]. **Agencia española de protección de datos – Directrices para la elaboración de contratos entre responsables y encargados del tratamiento -** https://www.aepd.es/media/guias/guia-directrices-contratos.pdf

[Ref - 20]. **Agencia española de protección de datos – Guía para el cumplimiento del deber de informar -** https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf

[Ref - 21]. **Agencia española de protección de datos - ¿Qué derechos tengo a partir del 25 de mayo de 2018? -** https://www.aepd.es/blog/2018-05-25.html

[Ref - 22]. **European Commission - Guidelines on Data Protection O icers ('DPOs') (wp243rev.01) -** https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

[Ref - 23]. **Agencia española de protección de datos – Guía práctica para las evaluaciones de impacto en la protección de los datos**

8

sujetas al RGPD - https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

[Ref - 24]. **INCIBE – Protege tu empresa – Herramientas de ciberseguridad – Políticas de seguridad para la pyme -** https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[Ref - 25]. **INCIBE – Protege tu empresa – Formación -** https://www.incibe.es/protege-tu-empresa/formacion

[Ref - 26]. **Enisa – Recomendations on shaping technology according to GDPR provisions -** https://www.aepd.es/media/docs/recomendations-on-shaping-technology-according-to-GDPR-provisions-1.pdf

[Ref - 27]. **arXiv.org - Security and Privacy Analyses of Internet of Things Children's Toys -** https://arxiv.org/pdf/1805.02751.pdf

[Ref - 28]. **OWASP – CheatSheetSeries -** https://github.com/OWASP/CheatSheetSeries/tree/master/cheatsheets

[Ref - 29]. **Enisa - Good practices for IoT and Smart Infrastructures Tool -** https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool

[Ref - 30]. **Iberley - Consentimiento de los menores de edad en materia de protección de datos en el Reglamento General de Protección de Datos (RGPD) y en la LO 3/2018 de 5 de diciembre (LOPDGDD) -** https://www.iberley.es/temas/consentimiento-menores-materia-proteccion-datos-62818

[Ref - 31]. **OWASP – Mobile app security checklist spanish -** https://github.com/OWASP/owasp-mstg/blob/master/Checklists/Mobile_App_Security_Checklist-Spanish_1.1.xlsx

[Ref - 32]. **Sans Institute – A security checklist for web application design -** https://www.sans.org/reading-room/whitepapers/securecode/security-checklist-web-application-design-1389

[Ref - 33]. **INCIBE – Guía – Glosario de términos de ciberseguridad -** https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf


GOBIERNO
DE ESPAÑA
MINISTERIO
DE ECONOMÍA
Y EMPRESA


incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD


protege
tu empresa


Asociación Española de
Fabricantes de Juguetes