Online Trust Alliance
an Internet Society initiative

Marco de confianza y confidencialidad de IoT v2.5

El Marco de confianza IoT (IoT Trust Framework®) incluye un juego de principios estratégicos necesarios para asegurar dispositivos IOT y sus datos cuando son enviados y a través de su ciclo de vida. A través de un proceso de múltiples actores impulsado por el consenso, se han identificado criterios para tecnologías conectadas del hogar, la oficina y prendas, incluidos juguetes, rastreadores de actividad y dispositivos de bienestar. El marco señala la necesidad de divulgaciones completas que deben ser provistas antes de la compra del producto, políticas respecto de la recolección, el uso, y como se comparten los datos, además de los términos y condiciones de los parches de seguridad post-garantía. Las actualizaciones de seguridad son esenciales para maximizar la protección de los dispositivos IoT a medida que se descubren vulnerabilidades y los ataques evolucionan. Adicionalmente, el marco proporciona recomendaciones para que los fabricantes mejoren la transparencia y la comunicación con respecto a la capacidad de recibir actualizaciones del dispositivo y una variedad de asuntos pertinentes a la privacidad de los datos.

La aplicación de los principios a la totalidad del ecosistema o armado de dispositivos es clave para abordar los riesgos de seguridad y los asuntos de privacidad inherentes. El ecosistema incluye el dispositivo o sensor, las aplicaciones de apoyo y servicios en la nube/de backend. Ya que tantos productos del mercado dependen de componentes y software de terceros o de código abierto, les corresponde a los desarrolladores aplicar estos principios y llevar a cabo evaluaciones de riesgos de seguridad y privacidad de la cadena de suministro.

Funcionando como una guía de evaluación para los desarrolladores, compradores y revendedores, el marco es la base para futuros programas de certificación de IoT. Es el objetivo de la OTA es señalar dispositivos que cumplen con estos estándares para ayudar a los consumidores, además de los sectores públicos y privados, a tomar decisiones de compra informadas. El marco y recursos relacionados se hallan disponibles en https://otalliance.org/IoT.

El marco puede dividirse en 4 áreas clave:

- **Principios de seguridad** (1-12) - Aplicable a cualquier dispositivo o sensor y todas las aplicaciones y servicios en la nube. Estos abarcan desde la aplicación de un proceso riguroso de seguridad de software a principios de seguridad de datos para datos almacenados y transmitidos por el dispositivo, hasta la gestión de la cadena de suministro, pruebas de penetración y programas de reporte de vulnerabilidad. Más principios delimitan los requisitos de parches de seguridad a lo largo del ciclo de vida.
- **Acceso y credenciales del usuario** (13-17) - Requisitos de encriptamiento de todas las contraseñas y nombres de usuario, envío de dispositivos con contraseñas únicas, implementación de procesos generalmente aceptados de restablecimiento de contraseñas e integración de mecanismos que ayuden a prevenir intentos de inicio de sesión mediante "fuerza bruta".
- **Privacidad, divulgaciones y transparencia** (18-33) - Requerimientos consistentes con principios de Privacidad generalmente aceptados, incluyendo divulgaciones prominentes en el envase, punto de venta y/o en línea, capacidad para que los usuarios puedan restablecer las configuraciones de fábrica y cumplimiento con requerimientos regulativos aplicables, incluido el EU GDPR y

regulaciones de Privacidad para niños. También aborda divulgaciones sobre el impacto que sufren las características o la funcionalidad del producto si la conectividad es inhabilitada.

- **Notificaciones y mejores prácticas relacionadas** (34-40) - Para mantener la seguridad del dispositivo es clave tener mecanismos y procesos que notifiquen rápidamente al usuario si hay una amenaza o una acción requerida. Los principios incluyen el requisito de autenticación por correo electrónico para notificaciones de seguridad y mensajes que sean claros y comprensibles para usuarios de todos los niveles de lectura. Adicionalmente, se destacan los requisitos de envasado seguro y accesibilidad.

OTA IoT Trust Framework® v2.5 – actualizado 14/10/17

Enfocado en dispositivos y servicios "para el consumidor" para el hogar y la empresa, incluyendo tecnología ponible

Marco de confianza IoT ● Requerido (Debe) ○ Recomendado (Debería)	
Seguridad - Dispositivo, aplicaciones y servicios en la nube	
1. Divulgue si el dispositivo es capaz de recibir actualizaciones de seguridad y, de ser así, divulgue si el dispositivo puede recibir actualizaciones de seguridad automáticamente y qué medidas debe tomar el usuario para asegurarse de que el dispositivo se actualice correctamente y a tiempo.	●
2. Asegúrese de que los dispositivos y las aplicaciones asociadas toleren los protocolos de criptografía y las mejores prácticas actuales generalmente aceptadas. Todos los datos de información personal en tránsito y almacenados deben estar encriptados empleando los estándares de seguridad actuales generalmente aceptados. Esto incluye, pero no se limita a conexiones alámbricas, Wi-Fi y Bluetooth.	●
3. Todos los sitios web de apoyo de IoT deben encriptar totalmente la sesión del usuario, desde el dispositivo hasta los servicios de backend. Las mejores prácticas actuales incluyen HTTPS y HTTP Strict Transport Security (HSTS) predeterminado, también conocido como AOSSL o Always On SSL. Los dispositivos deberían incluir mecanismos para autenticar confiablemente sus servicios de backend y aplicaciones de apoyo.[1]	●
4. Los sitios de apoyo de IoT deben implementar monitoreo regular y mejoras continuas en la seguridad del sitio y las configuraciones del servidor para reducir aceptablemente el impacto de vulnerabilidades. Realice pruebas de penetración al menos semestralmente.[2]	●
5. Establezca una divulgación coordinada de vulnerabilidad que incluya procesos y sistemas para recibir, rastrear y rápidamente responder a informes de vulnerabilidad externa de terceros, que incluyen, pero no se limitan a clientes, consumidores, el ámbito académico y la comunidad de investigación. Corrija vulnerabilidades de diseño posteriores a la puesta en el mercado de forma públicamente responsable ya sea a través de actualizaciones remotas y/o mediante notificaciones factibles al consumidor u otros mecanismos eficaces. Los desarrolladores deberían considerar los programas "bug bounty" y métodos de crowdsourcing para ayudar a identificar vulnerabilidades.	●
6. Asegúrese de que haya un mecanismo en funcionamiento para que métodos automatizados y seguros proporcionen actualizaciones de software y/o firmware, parches y revisiones. Tales actualizaciones deben ser firmadas y/o verificadas de otro modo como provenientes de una fuente confiable, incluyendo, pero no limitado al chequeo de firmas y de integridad.	●
7. Las actualizaciones y parches no deben modificar las preferencias, configuraciones de seguridad y/o privacidad configuradas por el usuario sin notificación previa. En casos en los que el firmware o software del dispositivo sean sobrescritos, primero se le debe dar al usuario la opción de revisar y seleccionar las configuraciones de privacidad.	●
8. Los procesos de actualizaciones de seguridad deben divulgar si son automatizadas (en lugar de automáticas). Las actualizaciones automatizadas le dan al usuario la habilidad de aprobar, autorizar o rechazar actualizaciones. En ciertos casos un usuario puede desear la habilidad de elegir como y cuando se realizan las actualizaciones, incluyendo, pero no limitado al consumo de datos y conexión a través de su operador de telefonía móvil o conexión ISP. A la inversa, las actualizaciones automáticas son impuestas al dispositivo sin interrupciones y sin interacción con el usuario y pueden o no brindar una notificación al usuario.	●

9. Asegúrese de que todos los dispositivos IoT y el software asociado han sido sujetos a pruebas rigurosas de desarrollo de software y ciclo de vida incluyendo pruebas de unidad, sistema, aceptación y regresión y modelado de amenazas, además de mantener un inventario de la fuente de cualquier código y/o componentes de terceros o de código abierto. Utilice una técnica de endurecimiento de códigos y sistemas generalmente aceptada abordando un rango de supuestos de uso cotidiano, incluyendo la prevención de pérdidas de datos entre el dispositivo, las aplicaciones y los servicios en la nube. Para desarrollar software seguro se debe pensar en la seguridad desde el comienzo del proyecto hasta su implementación, puesta a prueba y lanzamiento. Los dispositivos deberían enviarse con software actual y/o actualizaciones automáticas push en el primer encendido para abordar cualquier vulnerabilidad crítica conocida.	●
10. Lleve a cabo evaluaciones de riesgo de seguridad y de cumplimiento para todos los proveedores de servicios y de la nube. Vea la guía de recursos IoT https://otalliance.org/IoT	●
11. Desarrolle y mantenga una "lista de materiales" incluyendo software, firmware, hardware y bibliotecas de terceros (como módulos de código abierto y plug ins). Esto se aplica al dispositivo, los servicios móviles y los de la nube para ayudar a remediar vulnerabilidades informadas rápidamente.	○
12. Diseñe dispositivos con los requisitos mínimos necesarios para su operación. Por ejemplo, los puertos USB o ranuras para tarjetas de memoria solo deben incluirse si son necesarios para el funcionamiento y mantenimiento del dispositivo. Los puertos y servicios que no se usen deberían ser inhabilitados.	●
Credenciales y acceso del usuario	
13. Incluya autenticación fuerte predeterminada, que requiera brindar contraseñas únicas, generadas por el sistema o de un solo uso; o alternativamente use credenciales de certificado seguro. Donde sea necesario, requiera el uso de contraseñas únicas para el acceso administrativo, delimitando dispositivos y servicios y el respectivo impacto de los restablecimientos de fábrica.	●
14. Brinde mecanismos de recuperación generalmente aceptados para aplicaciones IoT y contraseñas de apoyo y/o mecanismos para el restablecimiento de credenciales empleando verificación y autenticación multi-factor (correo electrónico y teléfono, etc.) cuando no hay una contraseña de usuario.	●
15. Tome medidas para protegerse contra "fuerza bruta" y/u otros intentos de inicio de sesión agresivos (como bots de inicio de sesión automatizada, etc.) bloqueando o inhabilitando cuentas de apoyo de usuarios o dispositivos después de una cantidad razonable de intentos de inicio de sesión inválidos.	●
16. Brinde al os usuarios una notificación de cambio o restablecimiento de contraseña empleando autenticación segura y/o avisos fuera de banda.	●
17. Las credenciales de autenticación, incluyendo, pero no limitadas a contraseñas de usuarios, deben tener sal, una función hash y/o estar encriptadas. Se aplica a todas las credenciales guardadas para ayudar a prevenir el a acceso no autorizado y los ataques de fuerza bruta.	●
Privacidad, divulgaciones y transparencia	
18. Asegúrese de que las políticas de privacidad, seguridad y apoyo sean fáciles de encontrar y estén siempre disponibles para su revisión antes de la compra, activación, descarga o inscripción. Además de una colocación prominente en el envase del producto y en su sitio web, se recomienda a las empresas emplear códigos QR, url cortos y fáciles de usar y otros métodos similares en el punto de venta.	●
19. Divulgue la duración y el fin del ciclo de vida del soporte de seguridad y parches (pasada la garantía del producto). El apoyo puede terminar en una fecha determinada, como el 1 de enero de 2025, o luego un periodo de tiempo específico desde el momento de la compra, semejante a una garantía tradicional. Idealmente tales divulgaciones deberían alinearse con la vida útil esperada del	●

dispositivo y ser comunicadas al consumidor antes de la compra. *(Se reconoce que los dispositivos IoT no pueden ser seguros y aceptar parches indefinidamente. Considere comunicar los riesgos de usar un dispositivo luego del fin de su vida útil, y el impacto y el riesgo hacia los demás si las advertencias son ignoradas o el dispositivo no es dado de baja).* Si los usuarios deben pagar aranceles o suscribirse a un acuerdo de apoyo anual, esto debe divulgarse antes de la compra.	
20. Divulgue de manera visible qué datos de información personal y tipos de datos y atributos delicados se recolectan y cómo son utilizados, limitando la recolección a los datos que son razonablemente útiles para el funcionamiento y el propósito para el cual están siendo recolectados. Divulgue y brinde al consumidor la opción de compartir para cualquier otro propósito.	●
21. Divulgue qué características dejarán de funcionar y cómo lo harán si la conectividad o los servicios de backend son interrumpidos o inhabilitados, incluyendo, pero no limitado al potencial impacto sobre la seguridad física. Incluya lo que ocurre cuando el dispositivo ya no recibe actualizaciones de seguridad o si el usuario no actualiza el dispositivo. *(Considere incorporar controles para inhabilitar la conectividad o los puertos para mitigar potenciales amenazas, mientras mantenga la funcionalidad clave del producto, basándose en el uso del dispositivo, contrarrestando potenciales asuntos de vida/seguridad).*	●
22. Divulgue la política de retención de datos y la duración de almacenamiento de información personal.	●
23. Los dispositivos IoT deben enviar un aviso y/o solicitar la confirmación del usuario durante el primer aparejamiento, inducción y/o conexión con otros dispositivos, plataformas o servicios.	●
24. Divulgue si la posesión del dispositivo/producto/servicio IoT puede transferirse y cómo puede hacerse (ej., un hogar conectado vendido a un nuevo propietario o la venta de un monitor de actividad física).	●
25. Solo comparta los datos personales de los consumidores con terceros si tiene el consentimiento de los consumidores, a menos que sea requerido y limitado para el uso de características del producto o la operación del servicio. Requiera que los terceros proveedores de servicios estén sujetos a las mismas políticas, incluyendo mantener en confidencialidad dichos datos y el requisito de dar aviso en el caso de cualquier pérdida/violación de datos y/o acceso no autorizado.	●
26. Brinde controles y/o documentación para que el consumidor pueda revisar y editar las preferencias de privacidad del dispositivo IoT, incluida la posibilidad de "restablecer las configuraciones de fábrica".	●
27. Comprométase a no vender o transferir ningún dato de información personal de los consumidores a menos que sea una parte dependiente de la venta o liquidación de la empresa que originalmente recolectó los datos, solo si la política de privacidad de la parte adquisidora no cambia materialmente los términos. De no ser así debe darse aviso y solicitar consentimiento.	●
28. Brinde la posibilidad de que el consumidor devuelva el producto sin cargo luego de revisar las prácticas de privacidad que son presentadas antes del uso, si dichos términos no fueran visiblemente divulgados antes de la compra. El tiempo (número de días) para la devolución de un producto debe ser congruente con las políticas de cambio actuales del revendedor, o especificado de antemano.	●
29. Cuando sea que se presente la oportunidad de rechazar o no participar de una política, las consecuencias deben estar clara y objetivamente explicadas, incluido cualquier impacto en las características o funcionalidad del producto. Se recomienda que el valor para el usuario de participar y/o compartir datos se comunique al consumidor final.	●
30. Cumpla con regulaciones aplicables, incluyendo, pero no limitadas al Children's Online Privacy Protection Act (COPPA) y los requerimientos regulatorios internacionales de privacidad, seguridad y transferencia de datos.[3] [4]	●
31. Publique el historial de cambios materiales en el aviso de privacidad durante un mínimo de dos años. Las mejores prácticas incluyen poner el sello de la fecha, corregir y resumir el impacto de los cambios.	●
32. Brinde la posibilidad al usuario o proxy de eliminar, o hacer anónimos, datos personales o delicados almacenados en servidores de la empresa (que no sea el historial de la transacción de compra) al discontinuar el uso del dispositivo o si este se perdiera o se vendiera.	○

33. Brinde la posibilidad de restablecer el dispositivo a sus condiciones de fábrica, incluyendo la posibilidad de eliminar datos del usuario en caso de transferencia, alquiler, pérdida o venta.	O
Notificaciones y mejores prácticas relacionadas	
34. Las comunicaciones con el consumidor final, incluyendo, pero no limitadas a correo electrónico y SMS, deben adoptar protocolos de autenticación para ayudar a prevenir el spear-phishing y la suplantación. Los dominios deberían implementar SPF, DKIM y DMARC para todas las comunicaciones y avisos relacionados con la seguridad y la privacidad y también para dominios aparcados y aquellos que nunca envían correos electrónicos.[5]	●
35. Para comunicaciones por correo electrónico, dentro de los 180 días luego de haber publicado una política DMARC, implemente una política de rechazo o cuarentena, que a ayuda a los ISP y a las redes receptoras a rechazar correos electrónicos que no pasan los chequeos de autenticación de correo electrónico.[6]	O
36. Los vendedores de IoT que usen comunicación mediante correo electrónico deberían adoptar un nivel de confidencialidad de transporte, incluyendo técnicas de seguridad generalmente aceptadas para ayudar a que las comunicaciones sean seguras y a mejorar la privacidad e integridad del mensaje (también conocido como "TLS oportunista para correo electrónico").[7]	O
37. Implemente medidas para ayuda a prevenir o poner en evidencia cualquier manipulación física de los dispositivos. Tales medidas ayudan a proteger al dispositivo de ser abierto o modificado con intenciones maliciosas luego de su instalación o de ser devueltos al revendedor en un estado comprometido.	O
38. Considere como adaptarse a los requisitos de accesibilidad para usuarios que puedan tener discapacidades visuales, auditivas o motrices para maximizar el acceso para usuarios de todos los niveles de habilidad física.	O
39. Desarrolle procesos de comunicación para maximizar la sensibilización de los usuarios hacia cualquier problema potencial de seguridad o privacidad, hacia avisos de fin de la vida útil y posibles retiros de productos, incluyendo notificaciones dentro de la aplicación. Las comunicaciones deberían ser escritas para maximizar la comprensión en el nivel de lectura del usuario general. Considere las comunicaciones multilingües, reconociendo que el inglés puede ser el "segundo idioma" del usuario (vea los principios relacionados con respecto a la seguridad e integridad de los mensajes).	●
40. Promulgue un plan de respuesta ante violaciones y de aviso al consumidor que sea revaluado, probado y actualizado por lo menos anualmente y/o luego cambios significativos de sistema interno, técnicos y/u operacionales.	●

Recursos y actualizaciones publicados en https://otalliance.org/IoT

Terminología, definiciones y aclaraciones

1. Alcance - Enfocado en dispositivos y servicios "para el consumidor para el hogar y la empresa, incluyendo tecnología ponible." Los coches inteligentes, incluyendo vehículos autónomos, autoconducidos además de dispositivos médicos y datos HIPAA[8] están más allá del alcance del marco, pero la mayoría de los criterios se consideran aplicables. Entran bajo supervisión regulatoria del National Highway Traffic Safety Administration (NHTSA) y la Food and Drug Administration (FDA). [9]
2. Los términos fabricantes de dispositivos, vendedores, desarrolladores de aplicaciones, proveedores de servicios y operadores de plataformas se hallan todos indicados con el término "empresas".
3. Se espera que las empresas divulguen las instancias en las cuales compartan datos con la policía y que hagan referencia a cualquier informe de transparencia aplicable según sea permitido por la ley.
4. Los dispositivos inteligentes refieren a dispositivos y sensores que estén en una red y puede que solo tengan comunicaciones en un sentido.

[1] https://otalliance.org/resources/always-ssl-aossl

[2] https://otalliance.org/blog/responsible-coordinated-ethical-vulnerability-disclosures

[3] Las empresas, productos y servicios deben cumplir con todas las leyes o regulaciones de la jurisdicción que gobierne su recolección y manejo de información personal y delicada, incluyendo pero no limitado al respeto riguroso del Privacy Shield Framework de E.E.U.U.-UE www.commerce.gov/privacyshield y/o el General Data Protection Regulation (GDPR) de la Unión Europea www.eugdpr.org. El incumplimiento de estos puede constituir el incumplimiento de este marco.

[4] COPPA https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[5] Autenticación de correos electrónicos - https://otalliance.org/eauth

[6] DMARC -https://otalliance.org/resources/dmarc

[7] TLS for Email - https://otalliance.org/best-practices/transport-layered-security-tls-email

[8] Departamento de Salud y Servicios Sociales de los Estados Unidos, Privacidad de datos de salud http://www.hhs.gov/hipaa/index.html

[9] http://www.nhtsa.gov/Vehicle+Safety y http://www.fda.gov/MedicalDevices/default.htm

---

La OTA es una iniciativa dentro de Internet Society (ISOC), una organización sin fines de lucro benéfica 501c3 con la misión de promover el desarrollo, evolución y uso abierto de Internet para el beneficio de todas las personas alrededor del mundo. La misión de OTA es aumentar la confianza en línea, usar empoderamiento e innovación convocando iniciativas de múltiples actores, desarrollando y promocionando prácticas recomendadas, prácticas de privacidad responsables y administración de datos. Para aprender más visite https://otalliance.org y https://www.internetsociety.org.

R1014