INSTITUTO FEDERAL DE TELECOMUNICACIONES

CÓDIGO DE MEJORES PRÁCTICAS PARA LA **CIBERSEGURIDAD DE LOS DISPOSITIVOS** DEL INTERNET DE LAS COSAS (IOT)

Unidad de Política Regulatoria
Dirección General de Regulación Técnica
Diciembre 2022

ÍNDICE

1. Introducción

Como parte de la innovación y evolución tecnológica cada día hay más personas con acceso a Internet, así también dispositivos conectados a Internet; los productos y aparatos que tradicionalmente no se conectaban a Internet ahora lo están haciendo y necesitan ser diseñados para resistir amenazas en la seguridad.

Los riesgos vinculados a una falta o falla de seguridad de los dispositivos conectados a Internet afecta la confianza en la transformación digital y genera costos económicos y sociales, asimismo amenaza cada vez más la seguridad de las personas a través de dispositivos vulnerables del Internet de las cosas (IoT)[1].

La Asociación del Sistema Móvil Global (GSMA) a través del reporte *"La Economía Móvil América Latina 2019"* señala que las conexiones totales de los Dispositivos IoT en América Latina están creciendo en una tasa promedio anual de 14% y están en camino a alcanzar las 1300 millones de conexiones para 2025, lo que representa el 5% de las conexiones de IoT mundiales[2].

Aunado a lo anterior, en julio de 2021, SONICWALL publicó el reporte *"MID-YEAR UPDATE CYBER THREAT REPORT"*, en el que se estableció que en la primera mitad de 2021, se registraron 32,2 millones de intentos de malware a los dispositivos IoT, un incremento del 59 % durante el mismo año[3].

Actualmente, las personas confían sus datos personales a un número creciente de Dispositivos IoT y Servicios asociados en línea, que permanentemente están recolectando y compartiendo dichos datos; sin darse cuenta, las personas dan a conocer sus gustos, preferencias, horarios, direcciones, entre otras cosas, por lo que se deben valorar los datos personales que se comparten en la red y los riesgos que esto conlleva.

Por lo anterior, el presente documento toma como base la especificación técnica ETSI TS 103 645 V2.1.2 (2020-06) denominada *"CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements[4]"* la cual, fue elaborada por el Comité

---

[1] Organisation for Economic Co-operation and Development, Working Party on Security in the Digital Economy, ***Encouraging responsible vulnerability treatment: overview for policy makers.***

[2] https://www.gsma.com/r/mobileeconomy/latam-es/

[3] https://blog.sonicwall.com/en-us/2021/07/latest-cyber-threat-intelligence-shows-ransomware-skyrocketing/ Información complementaria obtenida de la conferencia *"Protección de Datos personales y Ciberseguridad"*, Dra. Cynthia Solís, IFT, noviembre 2021.

[4] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf

Técnico de Ciberseguridad (CYBER) del Instituto Europeo de Estándares de Telecomunicaciones (ETSI) donde se establecen las mejores prácticas internacionales en materia de ciberseguridad para los Dispositivos IoT.

El presente Código de mejores prácticas para la ciberseguridad del Internet de las Cosas (en lo sucesivo, "Código") es un instrumento de referencia, con el fin de coadyuvar a incentivar la innovación tecnológica en el sector de los Dispositivos IoT; retomando para ello mejores prácticas internacionales, con un enfoque basado en gestión de riesgos, enfatizando la seguridad por diseño.

Asimismo, busca fortalecer e impulsar el desarrollo del IoT en México y sus consecuentes beneficios sociales y económicos, así como el incremento de la confianza en el uso del Internet, coadyuvando a una evolución tecnológica segura y confiable, y la promoción de la responsabilidad social en el ecosistema digital.

Este Código se enfoca principalmente en los controles técnicos y las políticas organizativas más importantes para Dispositivos IoT que abordarán las deficiencias de seguridad más significativas y generalizadas; las recomendaciones se centran en resultados en lugar de ser prescriptivas.

No obstante lo anterior, el Instituto a efecto de incentivar la adopción del presente Código por Fabricantes de Dispositivos IoT, concesionarios y autorizados que brindan acceso a Internet, así como aquellos proveedores de aplicaciones, contenidos y/o servicio y cualquier otra persona física o moral que desarrolle y proporcione aplicaciones o servicios, será el encargado de la gestión de una base de datos de Dispositivos IoT y/o Servicios asociados, que almacenará cuales de éstos cumplen total o parcialmente con las recomendaciones establecidas en el Código en comento, especificando cada una de estas.

Lo anterior, beneficiará a los Fabricantes de Dispositivos IoT, concesionarios y autorizados que brindan acceso a Internet, y proveedores de aplicaciones, contenidos y/o servicio y cualquier otra persona física o moral que desarrolle y proporcione aplicaciones o servicios, a través de la difusión por medios electrónicos relativa a los Dispositivos IoT y Servicios asociados que dan cumplimiento al Código de mejores prácticas para la ciberseguridad de los dispositivos del Internet de las Cosas. Esto a su vez, empoderará al usuario final al hacer de su conocimiento la referida información, lo que también fomentará la libre elección y no discriminación en la selección de dichos Dispositivos IoT y servicios brindando mayor certeza en su adquisición y competencia en el sector del IoT.

2. Objetivo y campo de aplicación

El presente Código tiene por objetivo establecer recomendaciones de mejores prácticas de ciberseguridad para Dispositivos IoT, que puedan hacer uso del espectro radioeléctrico o ser conectados a redes de telecomunicaciones, los cuales se encuentran expuestos a amenazas, vulnerabilidades, riesgos y ataques dentro del ecosistema digital; así como para aquellos Servicios asociados que se encuentran vinculados a Dispositivos IoT que normalmente son requeridos para proporcionar la funcionalidad prevista por éstos. Lo anterior, con un enfoque basado en gestión de riesgos y enfatizando la seguridad por diseño.

Las recomendaciones de mejores prácticas contenidas en el presente Código están dirigidas a los Fabricantes de Dispositivos IoT, concesionarios y autorizados que brindan acceso a Internet, así como aquellos proveedores de aplicaciones, contenidos y/o servicio y cualquier otra persona física o moral que desarrolle y proporcione aplicaciones o servicios para los dispositivos en comento.

Los Dispositivos IoT que son empleados en procesos industriales, científicos o para fines médicos no están considerados dentro del campo de aplicación del presente Código.

3. Definiciones

Para efecto del presente Código, además de las definiciones previstas en la Ley Federal de Telecomunicaciones y Radiodifusión y demás disposiciones legales, reglamentarias y administrativas aplicables, se entenderá por:

I. **Administrador:** Usuario cuyo nivel de privilegios en la gestión del Dispositivo IoT le permite modificar la configuración de dicho dispositivo;

II. **Autenticación:** Acción de garantizar la identidad de una persona física o moral;

III. **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información, en los términos definidos en las leyes aplicables;

IV. **Dispositivo IoT:** En el Internet de las cosas, se trata de una pieza o componente de un equipo que pueda hacer uso del espectro radioeléctrico o ser conectado a redes de telecomunicaciones, los cuales se pueden emplear típicamente en el hogar o en dispositivos electrónicos portátiles, con capacidades opcionales de teledetección, accionamiento, captura, almacenamiento y/o procesamiento de datos y que guarda relación con un Servicio asociado a este;

V. **Dispositivo IoT restringido:** Dispositivo IoT con limitaciones físicas que restringen su capacidad para procesar, comunicar o almacenar información, o para interactuar con el usuario, derivado de las restricciones de su uso previsto. Estas limitaciones pueden estar en función de la fuente de alimentación, de la duración de la batería, de la capacidad de procesamiento, del acceso físico, de la capacidad de memoria o ancho de banda de la red;

VI. **Fabricante de Dispositivos IoT:** Persona física o moral que genera un Dispositivo IoT final ensamblado, el cual puede integrar productos y componentes de otros fabricantes y/o proveedores;

VII. **Módulo de seguridad:** Conjunto de "*hardware*", "*software*" y/o "*firmware*" que implementa las funciones de seguridad en un entorno de ejecución confiable;

VIII. **Interfaz de depuración:** Interfaz física utilizada por el Fabricante de Dispositivos IoT para comunicarse con el Dispositivo IoT durante el desarrollo o para realizar el control de pruebas de éste;

IX. **Interfaz lógica:** Implementación de "*software*" que utiliza una interfaz de red para comunicarse a través de la red mediante canales o puertos;

X. **Internet de las cosas (IoT):** Infraestructura mundial al servicio de la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión (física y virtual) de las cosas gracias al interfuncionamiento de tecnologías de la información y la comunicación (existentes y en evolución);

XI. **Parámetros críticos de seguridad:** Información secreta relacionada con la seguridad cuya divulgación o modificación puede comprometer un Módulo de seguridad, tales como las claves secretas criptográficas y valores de Autenticación como contraseñas, Número de Identificación Personal (NIP), así como los componentes privados de los certificados de seguridad;

XII. **Parámetros de seguridad sensibles:** Conjunto de Parámetros críticos de seguridad y de Parámetros públicos de seguridad;

XIII. **Parámetros públicos de seguridad:** Información pública relacionada con la seguridad cuya modificación puede comprometer el Módulo de seguridad, tales como una clave pública para verificar la autenticidad/integridad de las actualizaciones de "*software*", así como los componentes públicos de los certificados de seguridad;

XIV. **Servicios asociados:** Son aquellos servicios digitales proporcionados por los concesionarios y autorizados que brindan acceso a Internet, así como aquellos proveedores de aplicaciones, contenidos y/o servicio que se encuentran vinculados a los Dispositivos IoT y que normalmente son requeridos para proporcionar la funcionalidad prevista por éstos, y

XV. **Vulnerabilidades**: Fallo de seguridad que puede traducirse, intencional o accidentalmente, en una violación de la política de seguridad.

4. Abreviaturas

En el presente Código se emplean las siguientes abreviaturas:

API	Interfaz de Programación de Aplicaciones (del inglés, *Application Programming Interface*);
ARP	Protocolo de Resolución de Direcciones (del inglés, *Address Resolution Protocol*);
CVD	Divulgación Coordinada de Vulnerabilidades (del inglés, *Coordinated Vulnerability Disclosure*);
DDoS	Denegación de Servicio Distribuida (del inglés, *Distributed Denial of Service*);
DoS	Denegación de Servicio (del inglés, *Denial of Service*);
DHCP	Protocolo de Configuración Dinámica de Host (del inglés, *Dynamic Host Configuration Protocol*);
DNS	Sistema de Nombres de Dominio (del inglés, *Domain Name System*);
ICMP	Protocolo de Control de Mensajes de Internet (del inglés, *Internet Control Message Protocol*);
IEC	Comisión Electrotécnica Internacional (del inglés, *International Electrotechnical Commission);*
IoT	Internet de las Cosas (del inglés, *Internet of Things*);
ISO	Organización Internacional de Normalización (del inglés, *International Organization for Standardization*);

NTP	Protocolo de Tiempo en Red (del inglés, *Network Time Protocol*);
OTP	Contraseña de un Solo Uso (del inglés *One-Time Password*);
TEE	Entorno de Ejecución Confiable (del inglés, *Trusted Execution Environment*), y
UICC	Tarjeta de Circuito Integrado Universal (del inglés, *Universal Integrated Circuit Card*).

5. Recomendaciones y mejores prácticas

5.1 Sobre las contraseñas

5.1.1 Contraseñas únicas en Dispositivos IoT

Las contraseñas para los Dispositivos IoT en cualquier estado que no sea el predeterminado de fábrica podrán ser únicas o definidas por el usuario.

5.1.1.1 Consideraciones Adicionales

Los Dispositivos IoT nuevos con nombre de usuario y contraseña universal predeterminadas como ***"admin, admin"***, respectivamente, pueden causar problemas de seguridad a dichos dispositivos, así como a la red de telecomunicaciones en la que operan. Con el objetivo de evitar esta práctica, la seguridad de los Dispositivos IoT se puede fortalecer mediante el uso de contraseñas únicas preinstaladas en éstos y/o que requieren que el usuario elija una contraseña que siga las mejores prácticas como parte del proceso de su puesta en operación inicial, o por algún otro método que evite el uso de contraseñas.

La seguridad en los Dispositivos IoT, así como en los Servicios asociados puede incrementarse mediante el uso de la Autenticación de múltiples factores; es decir, empleando una contraseña adicional a un procedimiento OTP. Adicionalmente, la seguridad del Dispositivo IoT puede fortalecerse aún más si éste emplea identidades únicas e inmutables.

5.1.2 Contraseñas únicas preinstaladas en Dispositivos IoT

En caso de que el Dispositivo IoT haga uso de contraseñas únicas preinstaladas, estas podrán generarse mediante un mecanismo que reduzca el riesgo de ataques automatizados en contra de una clase o tipo

de Dispositivo IoT. Las contraseñas únicas preinstaladas podrán generarse de manera aleatoria.

5.1.3 Mecanismos de Autenticación

Los Dispositivos IoT que cuenten con mecanismos para la Autenticación de usuarios en éstos, tales como huella digital (biométricos), contraseñas u otros, podrán:

a) Emplear mejores prácticas en materia de criptografía, conforme a las propiedades de la tecnología, el riesgo y uso del Dispositivo IoT previsto;
b) Proporcionar al usuario o al Administrador un mecanismo simple para cambiar el valor de Autenticación empleado, y
c) Contar con mecanismos que eviten los ataques de fuerza bruta a los métodos de Autenticación a través de la interfaz de red de telecomunicaciones a la que se conecte el Dispositivo IoT. Lo anterior, es aplicable a Dispositivos IoT no restringidos.

5.2 Sobre la gestión de informes de vulnerabilidades

5.2.1 Información de contacto

Los Fabricantes de Dispositivos IoT podrán poner a disposición de sus usuarios una política de divulgación de vulnerabilidades que, al menos, considere lo siguiente:

a) Información de contacto para la notificación de vulnerabilidades, y
b) La información relativa a los plazos para:
    i. El acuse de notificación inicial de vulnerabilidades, y
    ii. La actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.

5.2.1.1 Consideraciones adicionales

Una política de divulgación de vulnerabilidades especifica el proceso mediante el cual los investigadores en seguridad y otros grupos interesados puedan aportar información sobre vulnerabilidades detectadas. Dicha política puede actualizarse conforme sea necesario para garantizar la transparencia y la claridad entre el Fabricante de Dispositivos IoT y los investigadores de seguridad y viceversa.

La CVD es un conjunto de procesos para abordar la difusión sobre las vulnerabilidades de seguridad y para apoyar la corrección de las éstas. Este proceso se encuentra estandarizado en la norma ISO/IEC 29147. Asimismo, proporciona un mecanismo para que los investigadores en seguridad puedan establecer una comunicación con los Fabricantes de Dispositivos IoT para informarles sobre los problemas de seguridad, colocando a éstos al frente de la amenaza, brindándoles la oportunidad para responder y resolver las vulnerabilidades antes de hacer una divulgación pública.

5.2.2 Tiempo de respuesta a vulnerabilidades divulgadas

Las vulnerabilidades divulgadas a los Fabricantes de Dispositivos IoT podrán ser atendidas oportunamente; el plazo promedio para el cierre de vulnerabilidades de "*software*" es de 90 días naturales.

5.2.3 Identificación y corrección de vulnerabilidades

Los Fabricantes de Dispositivos IoT o los proveedores de Servicios asociados podrán realizar un monitoreo continuo, por un periodo preestablecido, para identificar y corregir las vulnerabilidades de seguridad detectadas en los dispositivos o servicios que proporcionan, como parte del ciclo de vida útil de la seguridad de los dispositivos en comento; es importante mencionar que estas vulnerabilidades serán informadas a los usuarios.

NOTA: Es recomendable que los Fabricantes de Dispositivos IoT y los proveedores de Servicios asociados presten atención a todos los componentes de "*software*" y "*hardware*" proporcionados por un tercero que sean utilizados en los referidos dispositivos o servicios.

5.2.4 Divulgación de vulnerabilidades

Los Fabricantes de Dispositivos IoT podrán informar las vulnerabilidades de seguridad directamente a las partes afectadas en primera instancia. Si esto no es posible, podrán hacerlo a las autoridades nacionales competentes; adicionalmente, se fomentará la cooperación y coordinación entre las partes interesadas, lo anterior, para mitigar amenazas ante vulnerabilidades.

5.2.4.1 Consideraciones adicionales

Los informes de vulnerabilidades pueden comprender diferentes enfoques dependiendo de las circunstancias:

a) Vulnerabilidades relacionadas con productos o servicios: Las cuales podrán ser comunicadas directamente a la parte interesada afectada, como el Fabricante de Dispositivos IoT, el proveedor de Servicios asociados de IoT o el desarrollador de aplicaciones móviles. Las fuentes de estos informes pueden ser investigadores de seguridad o pares de la industria, y
b) Vulnerabilidades sistémicas: Una parte interesada, como un Fabricante de Dispositivos IoT, puede descubrir una vulnerabilidad que es potencialmente sistémica. Si bien, es crucial que el Fabricante del Dispositivo IoT corrija las fallas de éste, existe un beneficio significativo para la industria y los usuarios al compartir esta información. Del mismo modo, los investigadores en seguridad también pueden informar sobre estas vulnerabilidades sistémicas.

5.3 Sobre las actualizaciones de "*software*"

El desarrollo e implementación de actualizaciones de seguridad de *"software"* de forma oportuna es una de las acciones más importantes que los Fabricantes de Dispositivos IoT pueden tomar para proteger a sus usuarios y al ecosistema digital en general. A efecto de lo anterior, los Fabricantes de Dispositivos IoT y los proveedores de Servicios asociados podrán publicar una política sobre el término de la vida útil de los Dispositivos IoT en la que se indique de manera explícita la duración mínima del periodo durante el cual dicho dispositivo recibirá actualizaciones de *"software"*, y el motivo de la duración del periodo de asistencia. Además, indicará claramente para los usuarios finales la razón por la que cada actualización es necesaria.

Las vulnerabilidades a menudo provienen de componentes de *"software"* que no se prevé que guarden relación con la seguridad. Es una buena práctica que todo el *"software"* se mantenga actualizado y en buen estado.

5.3.1 Actualización segura

Los Fabricantes de Dispositivos IoT podrán actualizar de forma simple, segura y oportuna todos los componentes de "software" de los Dispositivos IoT que puedan hacer uso del espectro radioeléctrico o se conecten a la red de telecomunicaciones, sin afectar la función del dispositivo en comento. Lo

anterior, observando el término de la vida útil de los Dispositivos IoT indicada en el numeral anterior.

Se podrá garantizar la procedencia e instalación de las actualizaciones de "software" a través de mecanismos seguros que utilicen las mejores prácticas de criptografía.

5.3.1.1 Consideraciones adicionales

La periodicidad de las actualizaciones de *"software"* puede variar, dependiendo del problema particular y de la solución, así como de otros factores, como la capacidad de conexión del Dispositivo IoT o las consideraciones de un Dispositivo IoT restringido.

Es preciso señalar que, las actualizaciones de seguridad que corrijan vulnerabilidades críticas, es decir, aquellas que tienen efectos potencialmente adversos a gran escala, podrán ser manejadas con la prioridad apropiada por los Fabricantes de Dispositivos IoT y/o proveedores de Servicios asociados.

5.3.2 Automatización de las actualizaciones

En caso de que los Dispositivos IoT cuenten con todos los elementos que permitan utilizar mecanismos automáticos para las actualizaciones de "*software*", éstos últimos podrán estar habilitados y activos para los usuarios; asimismo podrán ser configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.

Aunado a lo anterior, los Dispositivos IoT, así como los Servicios asociados posterior a su puesta en operación inicial, podrán revisarse periódicamente si cuentan con alguna actualización de seguridad.

5.3.2.1 Consideraciones adicionales

Las actualizaciones de seguridad de *"software"* pueden ser proporcionadas a los Dispositivos IoT de manera preventiva, a menudo como parte de las actualizaciones automáticas, que pueden eliminar las vulnerabilidades de seguridad antes de que éstas se ejecuten. Esta gestión puede ser compleja, especialmente si hay que lidiar con actualizaciones de *"software"* paralelas de servicios en la nube, actualizaciones de dispositivos y otras actualizaciones de Servicios asociados. Por lo tanto, los Fabricantes de

Dispositivos IoT, así como los proveedores de Servicios asociados podrán contar con un plan de gestión y despliegue que sea transparente para los usuarios acerca el estado actual del soporte de actualización.

En muchos casos, la publicación de actualizaciones de *"software"* conlleva una interdependencia con otras organizaciones, como los fabricantes de subcomponentes; sin embargo, esta no es una razón para no ejecutar las actualizaciones de *"software"*. Es preciso indicar que toda la cadena de suministro de *"software"* podrá ser considerada en el desarrollo e implementación de las actualizaciones de seguridad.

5.3.3 Autenticidad e integridad de las actualizaciones

El Dispositivo IoT podrá constatar la autenticidad e integridad de las actualizaciones del *"software"*.

NOTA: En caso de Dispositivos IoT restringidos, la Autenticación podrá llevarse a cabo mediante un dispositivo auxiliar que realice dicha verificación.

5.3.4 Divulgación de las actualizaciones

Los Fabricantes de Dispositivos IoT podrán informar a los usuarios sobre el requerimiento de actualizaciones de manera oportuna; dichas actualizaciones contendrán de forma clara la información de los riesgos a mitigar, conforme a la política de vida útil arriba indicada la cual deberá de fácil implementación por los usuarios.

5.3.5 Continuidad de las funciones

El Dispositivo IoT podrá notificar al usuario cuando se aplique una actualización de *"software"* que interrumpa de forma temporal el funcionamiento básico de éste. Particularmente para aquellos dispositivos que cumplen una función relevante de seguridad, el funcionamiento básico del Dispositivo IoT, podrá mantenerse durante las actualizaciones de *"software"*.

5.3.6 Dispositivos IoT restringidos

Para los Dispositivos IoT restringidos que no pueden actualizar su propio *"software"* se podrá considerar:

a) Que estos sean aislables y el *"hardware"* reemplazable, y
b) Que los Fabricantes de Dispositivos IoT publiquen de manera accesible, clara y transparente para el usuario la justificación de la ausencia de actualizaciones de *"software"*, el periodo de soporte de reemplazo de *"hardware"*, así como la política de fin de vida útil.

5.3.7 Etiquetas para Dispositivos IoT

El modelo del Dispositivo IoT podrá ser fácilmente identificable a través del etiquetado en éste o mediante su interfaz física, con el objetivo de constatar la disponibilidad y el periodo de soporte definido para las actualizaciones de "*software*".

5.4 Sobre las credenciales y los Parámetros de seguridad sensibles

5.4.1 Almacenamiento seguro

El Dispositivo IoT podrá utilizar mecanismos de almacenamiento seguro para proteger los Parámetros de seguridad sensibles. Entre estos se encuentran el TEE, así como capacidades de procesamiento de "*software*" en UICC.

5.4.1.1 Consideraciones adicionales

Los Fabricantes de Dispositivos IoT, pueden hacer uso de mecanismos de almacenamiento seguro en la memoria para los Parámetros de seguridad sensibles.

5.4.2 Credenciales Únicas y Codificadas

a) En caso de que el Dispositivo IoT emplee credenciales codificadas con fines de seguridad, se podrán implementar de manera que sean resistentes a la manipulación por medios físicos, electrónicos o informáticos, y
b) Los Dispositivo IoT no podrán admitir Parámetros de seguridad críticos codificados en el "*software*" de éste.

5.4.2.1 Consideraciones adicionales

Mediante el uso de ingeniería inversa se pueden descubrir fácilmente credenciales codificadas en el "*software*" de los Dispositivos IoT y aplicaciones, tales como nombres de usuario y contraseñas. Por otro lado,

los métodos de ofuscación simple también son empleados para ocultar o cifrar esta información.

5.4.3 Integridad y autenticidad de parámetros sensibles

Los Dispositivos IoT podrán emplear Parámetros críticos de seguridad para comprobar la integridad y la autenticidad de las actualizaciones de *"software"* así como para proteger la comunicación de los Servicios asociados con éste; dichos Parámetros serán únicos y generados con un mecanismo que reduzca el riesgo de ataques automatizados en contra de estos Dispositivos.

5.5 Sobre el uso de comunicaciones seguras

5.5.1 Cifrado de las comunicaciones

Los Dispositivos IoT podrán:

a) Emplear las mejores prácticas en materia de criptografía para comunicaciones seguras;
b) Emplear algoritmos y prácticas criptográficas actualizables, y
c) Prever que en el caso de que no puedan actualizarse, la vida útil prevista para este no excederá el periodo recomendado para los algoritmos criptográficos.

5.5.1.1 Consideraciones adicionales

Los Dispositivos IoT podrán ser resistentes a ataques en el cifrado de éstos. La idoneidad de los controles de seguridad y cifrado dependen de múltiples factores, incluido el contexto de uso.

5.5.2 Gestión de las claves de cifrado

Las claves de cifrado para los Dispositivos IoT y los Servicios asociados podrán gestionarse de forma segura.

5.5.3 Interfaz de red

Los Dispositivos IoT en su puesta inicial de operación, podrán permitir cambios relevantes a la configuración de seguridad a través de la interfaz de red una

vez que éste se haya autenticado; quedan exentos los protocolos de servicio de red como ARP, DHCP, DNS, ICMP, y NTP, ya que el Fabricante de los Dispositivos IoT no puede garantizar la configuración necesaria para que el dispositivo en mención funcione correctamente.

El Dispositivo IoT podrá proteger la confidencialidad de los Parámetros críticos de seguridad que sean transmitidos a través de interfaces de red accesibles de forma remota.

5.5.4 Parámetros críticos de seguridad

Los Fabricantes de Dispositivos IoT podrán cifrar los Parámetros críticos de seguridad durante la transmisión, mediante mecanismos de cifrado adecuados a las propiedades de la tecnología, los riesgos y el uso de éstos.

5.5.5 Estándares Abiertos

Los Dispositivos IoT podrán usar estándares abiertos y revisados entre pares que trabajan en el mismo campo.

5.6 Sobre las superficies expuestas a ataques

5.6.1 En "s*oftware*"

Los Dispositivos IoT podrán funcionar bajo el *"principio de privilegio mínimo"*[5] de conformidad con lo siguiente:

a) Las interfaces de red, así como las Interfaces lógicas que no se encuentren en operación podrán ser deshabilitadas;
b) Los servicios de *"software"* si no son empleados no estarán disponibles;
c) El *"software"* podrá limitarse a la funcionalidad requerida para que el Dispositivo IoT o el Servicio asociado funcionen correctamente;
d) El *"software"* podrá ejecutarse con los privilegios mínimos necesarios, teniendo en cuenta tanto la seguridad como la funcionalidad;
e) En el estado de inicio de operación, las interfaces de red del Dispositivo IoT podrán limitar la difusión no autenticada de información relevante para la seguridad;

[5] *Este principio es la base de una buena ingeniería de seguridad, aplicable tanto a IoT como a cualquier otro campo.*

f) La Interfaz de depuración podrá ser desactivada mediante el "*software*", y
g) El Fabricante de Dispositivos IoT podrá seguir los procesos de desarrollo seguro para el "*software*" empleado en éste.

5.6.2 En "*hardware*"

a) Los Fabricantes de Dispositivos IoT podrán establecer que: El "*hardware*" del Dispositivo IoT no otorgará accesos innecesarios a los puertos seriales, de red o puntos de prueba, que podrían derivar en un ataque, y
b) El Dispositivo IoT podrá incluir un mecanismo de control de acceso a nivel de "*hardware*" para la memoria, a efecto de evitar la ejecución de código malicioso.

5.7 Sobre la integridad del "*software*"

5.7.1 Inicio seguro

El "*software*" de los Dispositivos IoT podrá verificarse mediante mecanismos de inicio seguro, los cuales requieren un Módulo de seguridad en el "*hardware*".

5.7.2 Cambios no autorizados al "*software*"

Si el Dispositivo IoT detecta un cambio no autorizado en su "*software*", podrá alertar al usuario y al Administrador de la red sobre el incidente detectado y no podrá conectarse a redes más allá de las necesarias para realizar la función de alerta.

5.7.2.1 Consideraciones adicionales

La capacidad de recuperación de forma remota ante las situaciones anteriores, podrá partir de un estado de funcionamiento adecuado conocido, como un almacenamiento local de una versión con un estado de funcionamiento óptimo, para usarla como actualización y recuperación segura en el Dispositivo IoT. Esto evitará la DoS, retiro de los Dispositivos IoT o visitas de mantenimiento, a la vez que se gestiona el riesgo de que un atacante tome el control del referido dispositivo alterando la actualización u otros mecanismos de comunicación con la red de telecomunicaciones.

Si un Dispositivo IoT detecta que ha ocurrido algo inusual en su *"software"*, podrá informarlo a la persona apropiada; en estos casos, una alerta al Administrador de la red de telecomunicaciones, quien es la persona que tiene la capacidad de actuar ante la alerta.

5.8 Sobre la protección de los Datos personales

5.8.1 Confidencialidad de los Datos personales

La confidencialidad de los Datos personales transmitidos entre los Dispositivos IoT y los proveedores de Servicios asociados podrán protegerse mediante las mejores prácticas de criptografía, conforme a las propiedades de la tecnología, el riesgo y uso del Dispositivo IoT y de conformidad con la legislación que en materia de datos personales resulte aplicable.

5.8.2 Información clara y transparente

Los Fabricantes de Dispositivos IoT y los proveedores de Servicios asociados deberán proporcionar a los usuarios información clara y transparente sobre cómo se utilizarán sus Datos personales, quién los utilizará y con qué fines, por Dispositivo IoT y en cada Servicio asociado, de conformidad con la legislación que en materia de datos personales resulte aplicable. Esto también podrá resultar aplicable a terceras partes que puedan estar involucradas, como los anunciantes.

5.8.3 Consentimiento de los usuarios

a) Para el tratamiento de los Datos personales se requiere del consentimiento de los usuarios, de acuerdo con las formalidades previstas en la legislación que en materia de protección de datos personales resulte aplicable.

b) Los usuarios que hayan otorgado su consentimiento a los Fabricantes de Dispositivos IoT y a los proveedores de Servicios asociados para el uso de sus Datos personales deberán tener la oportunidad de revocarlo en cualquier momento, pudiéndose realizar a través de medios electrónicos cuando así lo haya aceptado expresamente el interesado. El Fabricante del Dispositivo IoT y los proveedores de Servicios asociados, garantizarán que los Datos personales sean tratados de conformidad con la legislación que en materia de protección de datos personales resulte aplicable.

La obtención del consentimiento del usuario se deberá realizar de conformidad con la normatividad aplicable en materia de protección de datos personales. En caso de que el responsable del tratamiento de los Datos personales pretenda darles un uso distinto para el cual el titular otorgó su consentimiento, este debe de ser recabado nuevamente; se deberán proporcionar a los usuarios los medios para preservar la privacidad de éstos mediante la configuración del Dispositivo IoT y la adecuada funcionalidad de los Servicios asociados y de conformidad con la legislación que en materia de protección de datos personales resulte aplicable.

5.9 Sobre la resiliencia a interrupciones

5.9.1 Interrupciones en la red telecomunicaciones y en la red de energía eléctrica

La resiliencia podrá integrarse en los Dispositivos IoT y en los Servicios asociados, cuando así lo requiera su uso u otros sistemas que los utilicen; considerando la posibilidad de interrupciones en la red de telecomunicaciones y en la red de energía eléctrica.

5.9.2 Operación durante las interrupciones

Los Dispositivos de IoT y los Servicios asociados podrán permanecer en operación y localmente funcionales, en el caso de una desconexión a la red de telecomunicaciones y podrán recuperarse de manera transparente después de un corte de energía eléctrica.

5.9.3 Reconexión

Los Dispositivos IoT en caso de una desconexión, podrán conectarse a la red de telecomunicaciones en un estado óptimo, operativo y estable, así como de forma ordenada, en lugar de una reconexión a gran escala.

5.9.3.1 Consideraciones adicionales

Los usuarios confían en los sistemas y Dispositivos IoT para usos prácticos cada vez más importantes que pueden ser relevantes para la seguridad o tener un impacto en sus vidas. Mantener los servicios activos en un ámbito local, en caso de una desconexión con la red de telecomunicaciones, es una de las

medidas que pueden ser tomadas para aumentar la resiliencia. Otras medidas pueden incluir la creación de redundancia de conexiones a otros Servicios asociados, así como mitigaciones contra ataques de DDoS que pueden ser causadas por conexiones masivas de dispositivos después de una interrupción. El nivel de resiliencia necesario podrá ser proporcional y estar determinado por el uso, teniendo en cuenta a otros que puedan depender del sistema, servicio o Dispositivo IoT, dado que una interrupción puede tener un impacto mayor del esperado.

Lo anterior, tiene como objetivo garantizar que los Servicios asociados de IoT se mantengan en operación, incluso en las funciones que son relevantes para la seguridad personal.

5.10 Sobre los datos de telemetría

5.10.1 Análisis de los datos de telemetría

Los datos de telemetría recopilados de los Dispositivos IoT o de los Servicios asociados, como los datos de uso y medición de éstos, podrán ser examinados para identificar entre otros, anomalías en la seguridad.

NOTA: La supervisión de telemetría, incluidos los datos de registro, es útil para la evaluación de la seguridad; identifica y resuelve circunstancias inusuales de manera temprana, minimizando el riesgo de seguridad y permitiendo una rápida mitigación de las éstas.

5.10.2 Contenido y uso de los datos de telemetría

Para los datos de telemetría recopilados de los Dispositivos IoT o de Servicios asociados considerará lo siguiente:

a) Que el periodo de tratamiento de los Datos personales deberá ser el mínimo indispensable y de conformidad con la legislación en materia de protección de datos aplicable, y
b) Que se podrá proporcionar a los usuarios información sobre los datos de telemetría recopilados y los motivos de ello.

5.11 Sobre la eliminación de Datos personales (Configuración)

Los Dispositivos IoT y los Servicios asociados podrán configurarse de manera que los Datos personales puedan ser eliminados en su caso total o parcialmente:

a) Fácilmente por el usuario;
b) En el caso de una transferencia de la propiedad a otro usuario del Dispositivo IoT o de los Servicios asociados;
c) Cuando el usuario elimine un Servicio asociado del Dispositivo IoT, y
d) Cuando el Dispositivo IoT llegue al fin de su vida útil.

5.11.1 Instrucciones y confirmación de eliminación

a) Los Fabricantes de Dispositivos IoT o los proveedores de Servicios asociados podrán proporcionar instrucciones claras al usuario sobre cómo eliminar los Datos personales registrados, y
b) Los Fabricantes de Dispositivos IoT o los proveedores de Servicios asociados podrán proporcionar al usuario una confirmación clara de que sus Datos personales han sido eliminados de los Dispositivos IoT o los Servicios asociados.

5.11.1.1 Consideraciones adicionales

Los Dispositivos IoT suelen cambiar de propietario y eventualmente se reciclan o se desechan, por ello, se podrán generar mecanismos que permitan al usuario eliminar sus Datos personales de los Dispositivos IoT y Servicios asociados, ya que la eliminación no se logra simplemente restableciéndolo a sus valores de fábrica predeterminados.

Asimismo, cuando un usuario desee eliminar completamente sus Datos personales de los Dispositivos IoT o Servicios asociados, se podrán incluir las copias de respaldo que, en su caso, el proveedor de Servicios asociados pudiera tener.

5.12 Sobre la instalación y el mantenimiento

5.12.1 Indicaciones claras y precisas

La instalación y mantenimiento de los Dispositivos IoT empleará el menor número de pasos y seguir las mejores prácticas en materia de seguridad. Los Fabricantes de Dispositivos IoT podrán proveer a los usuarios indicaciones claras y precisas sobre la configuración y constatación de que el Dispositivo IoT esté configurado de forma segura y automática.

5.12.1.1 Consideraciones adicionales

Los incidentes de seguridad causados por una configuración errónea o por la confusión del usuario pueden ser reducidos y, frecuentemente eliminados, si se da un manejo adecuado a la complejidad y al diseño en las interfaces de usuario.

5.13 Sobre la validación de los datos de entrada

5.13.1 Validación de las entradas

El "*software*" del Dispositivo IoT y los Servicios asociados podrán validar el ingreso de datos a través de las interfaces de usuario o de las transferencias entre las redes y los Servicios asociados mediante las API.

5.13.1.1 Consideraciones adicionales

Los sistemas pueden ser alterados mediante datos con formato incorrecto o código transferido a través de diferentes tipos de interfaz. Los atacantes suelen utilizar herramientas automatizadas para aprovechar las posibles amenazas y vulnerabilidades que surgen como resultado de la falta de validación de los datos. Los ejemplos incluyen, pero no se limitan a datos que:

a) No son del tipo de dato esperado, y
b) Están fuera del intervalo válido.

6 Bibliografía

(1) ETSI TS 103 645 V1.1.1. "*CYBER; Cyber Security for Consumer Internet of Things.*" Feb 2019.
(2) ETSI TS 103 645 V2.1.2. "*CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements.*" Jun 2020.
(3) *Department for Digital, Culture, Media & Sport*. "*Code of Practice for Consumer IoT Security.*" *United Kingdom*. Oct 2018.
(4) NIST, Special Publication 800-63B: "*Digital Identity Guidelines - Authentication and Lifecycle Management.*" Jun 2017.
(5) ISO/IEC 29147: 2018. "*Information technology — Security techniques — Vulnerability disclosure*". Oct 2018.
(6) IoT *Security Foundation*. "*Vulnerability Disclosure Guidelines* (*Release* 1.1)." Dec 2017.
(7) ETSI TR 103 331: "*CYBER; Structured threat information sharing.*" Aug 2016.

7 Concordancia con recomendaciones internacionales

El presente Código concuerda parcialmente con la especificación técnica ETSI TS 103 645 V1.1.1 y con la especificación técnica ETSI TS 103 645 V2.1.2.

ift INSTITUTO FEDERAL DE TELECOMUNICACIONES

CÓDIGO DE MEJORES PRÁCTICAS PARA LA **CIBERSEGURIDAD DE LOS DISPOSITIVOS** DEL INTERNET DE LAS COSAS (IOT)

Instituto Federal de Telecomunicaciones
Insurgentes Sur #1143 Col. Nochebuena
Demarcación Territorial Benito Juárez
C.P. 03720 Ciudad de México
Tel: 55 5015 4000 / 800 2000 120

www.ift.org.mx