ift INSTITUTO FEDERAL DE TELECOMUNICACIONES

CÓDIGO DE MEJORES PRÁCTICAS **PARA LA CIBERSEGURIDAD EN** EQUIPOS TERMINALES MÓVILES

Unidad de Política Regulatoria
Dirección General de Regulación Técnica
Diciembre 2022

Índice

1. Introducción

El creciente interés en la ciberseguridad está impulsado por el continuo desarrollo de los Equipos Terminales Móviles (ETM) en el mercado; sin embargo, la sofisticación y la rapidez de los avances tecnológicos en materia de movilidad va acompañada de la evolución de las amenazas, vulnerabilidades, riesgos y ataques en contra de los ETM, las redes públicas de telecomunicaciones, las aplicaciones móviles y la cadena de suministro de la tecnología en el ecosistema móvil en general.

Es relevante mencionar, que actualmente hay más ETM en los Estados Unidos de América que personas y el porcentaje de usuarios de ETM continúa creciendo drásticamente. En ese sentido, se estimó que en Estados Unidos de América había cerca de 236 millones de ETM en el año 2019,[1] mientras que en México se estimaron 115.8 millones de ETM a finales del 2020.[2]

Los ETM permiten a los usuarios finales acceder a información y a los servicios de telecomunicaciones en cualquier momento y lugar, tanto para uso personal, así como para asuntos laborales y de entretenimiento; pequeños, portátiles, conectados en todo momento, los ETM permiten el acceso instantáneo a Internet y a un conjunto diverso de aplicaciones móviles.

Sin embargo, un detalle muy importante que quizás la mayoría de los usuarios finales desconocen es que los ETM, representan una de las mayores superficies de ataque (ver definición) por el interés que genera la información personal contenida en éstos, la cual es proporcionada por los usuarios cuando emplean las aplicaciones móviles instaladas en dichos ETM y que brindan acceso, entre otros, al sistema financiero, correo electrónico, redes sociales y mensajes de texto; información que, a su vez, pueden emplearse para la suplantación de identidad, fraude u otros delitos.

Por otro lado, y derivado del tamaño y forma de los ETM, éstos permiten a los usuarios finales un fácil manejo y transporte, lo que los hace más propensos a ser extraviados o robados; adicionalmente, los ETM al estar permanentemente conectados a las redes públicas de telecomunicaciones o a otros dispositivos a través de múltiples interfaces de conexión tales como, Wi-Fi, Bluetooth, GNSS, NFC, (ver abreviaturas) etc., son propensos a amenazas, vulnerabilidades, riesgos y ataques dentro del ecosistema móvil.

En noviembre del 2017, *Harvard Business Review* (HBR), en su informe denominado *"Hackers Are Targeting Your Mobile Phone. Here Are 15 Ways to Slow Them Down"*[3] señaló que la ciberseguridad aplicada a los ETM se estaba convirtiendo en una preocupación y estimó que el costo de los ataques a las aplicaciones móviles alcanzaría $ 1.5 mil millones de dólares en el 2021. Lo anterior, derivado de que la ciberseguridad aplicada a los ETM no ha recibido la misma atención que la seguridad en

[1] https://es.statista.com/estadisticas/634136/usuarios-de-telefonos-inteligentes-en-los-estados-unidos-2010-2019/
[2] https://www.theciu.com/publicaciones-2/2021/4/5/mercado-de-smartphones-en-mxico-2020-una-vista-por-fabricante-de-equipos
[3] https://hbr.org/2017/11/hackers-are-targeting-your-mobile-phone-here-are-15-ways-to-slow-them-down)

los sistemas de red y de computadoras personales; HBR informó que el gasto en ciberseguridad en 2016 para ETM presentó un rezago en comparación con el gasto que se destina al desarrollo de aplicaciones móviles, un ejemplo de lo anterior es el gasto de 34 millones de dólares anuales que se dedicaron al desarrollo de aplicaciones móviles, comparado con los 2 millones de dólares para la seguridad en ETM.

Es así como, a efecto de coadyuvar a la seguridad de la información de los usuarios finales en los ETM y en las redes de telecomunicaciones móviles, el presente *"Código de mejores prácticas para la ciberseguridad en Equipos Terminales Móviles"* (Código) recopila recomendaciones de mejores prácticas en materia de ciberseguridad, considerando como base los siguientes instrumentos internacionales:

I. El estudio denominado *"Study on Mobile Device Security"*[4], elaborado por el departamento de seguridad nacional de los Estados Unidos de América y
II. El reporte intitulado *"Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions"*[5] elaborado por la Unión International de Telecomunicaciones a través de la iniciativa "*Financial Inclusion Global Initiative*" del año 2020.

Este Código se enfoca principalmente en los controles técnicos y políticas organizativas más importantes para ETM, abordando las deficiencias de seguridad más significativas y generalizadas; sus recomendaciones se centran en resultados en lugar de ser prescriptivas.

No obstante lo anterior, a efecto de incentivar la adopción del presente Código por parte de los usuarios finales, fabricantes de ETM, por personas físicas o morales que desarrollen y proporcionen servicios y aplicaciones, así como por los concesionarios y autorizados del servicio móvil (Operadores), el Instituto Federal de Telecomunicaciones (Instituto) podrá gestionar una base de datos de ETM, que almacenará información en un formato homologado, proporcionada periódica y voluntariamente por parte de los involucrados e interesados en el desarrollo de la seguridad de los ETM; dicha base de datos indicará de manera detallada qué ETM siguen total o parcialmente las recomendaciones establecidas en el presente Código.

Esta información podrá estar disponible y ser difundida por el Instituto (en sus redes sociales y en su portal de Internet), a efecto de dar a conocer a los usuarios finales qué ETM siguen las recomendaciones establecidas en el presente, lo que favorecerá la libre elección de los referidos ETM, brindando mayor certeza al momento de su adquisición y favoreciendo la competencia en el sector de las telecomunicaciones.

Aunado a lo anterior, el Código en comento pretende crear e impulsar una cultura y conciencia en los usuarios finales, sobre el uso y cuidado responsable de la información personal contenida en los ETM.

[4] https://www.dhs.gov/publication/st-mobile-device-security-study

[5] https://www.itu.int/en/ITUT/extcoop/figisymposium/Documents/Technical%20report%20on%20SS7%20vulnerabilities%20and%20mitigation%20measures%20for%20Digital%20Financial%20Services%20transactions.pdf

2. Objetivo y Campo de aplicación

El presente Código tiene como objetivo emitir recomendaciones de mejores prácticas en materia de ciberseguridad para los ETM 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 móvil.

Las recomendaciones de mejores prácticas contenidas en el presente Código están dirigidas a los usuarios finales, fabricantes de ETM, a las personas físicas o morales que desarrollen y proporcionen servicios y aplicaciones para los ETM, así como a los Operadores; lo anterior, a efecto de ser adoptadas e implementadas en el uso, fabricación y operación de los ETM, con el objeto de coadyuvar a proteger a los usuarios finales mediante la mitigación de amenazas, vulnerabilidades, riesgos y ataques de los que son objeto los ETM en el ecosistema móvil; lo anterior empleando un enfoque basado en gestión de riesgos y enfatizando la seguridad por diseño.

En ese sentido, el presente Código se centra en recomendaciones enfocadas a las superficies de ataque del *hardware* y del *software* de los ETM; sin embargo, también se enuncian de manera general algunas otras recomendaciones aplicables a otras superficies de ataque.

El presente Código no considera dentro del campo de aplicación, los dispositivos IoT, los Sistemas De Control de Supervisión y Adquisición de Datos (SCADA), los sistemas de control industrial, las interfaces celulares que operan como subsistemas (plataformas) como en los sistemas de entretenimiento de sistemas automotrices o en electrodomésticos.

3. Definiciones

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

I. **Activo:** Cualquier elemento (cosa) que tenga valor para un individuo, organización o para un gobierno.[6]
II. **Amenaza:** Causa potencial de un incidente indeseado, que puede infringir daño a un sistema u organización.[7]
III. **Atacante:** Persona que se introduce ilegalmente en los sistemas con la intención de realizar Ataques Pasivos o Activos.[8]

[6] *International Standard ISO/IEC 27032, Information technology — Security techniques — Guidelines for cybersecurity*
[7] https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1127-201709-I!!PDF
[8] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2007-PDF-S.pdf

IV. **Ataques Activos**: Ataque que modifica los recursos objeto del ataque (con perjuicio de los criterios de integridad, disponibilidad y confidencialidad).[9]

V. **Ataques de diccionario:** Método empleado para romper la seguridad de los sistemas basados en contraseñas en la que el Atacante intenta dar con la clave adecuada probando todas (o casi todas) las palabras posibles en un diccionario idiomático.[10]

VI. **Ataques de Fuerza Bruta:** Ataque que implica probar todas las combinaciones posibles para encontrar una coincidencia.[11]

VII. **Ataques Pasivos**: Se presenta cuando un Atacante vulnera el mecanismo de autenticación e intercepta la información transmitida por la red de telecomunicaciones, sin que éste la modifique.[12]

VIII. ***Botnet***: Red compuesta por ETM infectados con *Malware,* controlados a distancia, por medio de un servidor de control operado por un Atacante.[13]

IX. ***Bluetooth***: Protocolo inalámbrico que permite que dos dispositivos equipados de manera similar se comuniquen entre sí dentro de una distancia corta[14]

X. **Ciberseguridad:** Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los Activos de los Usuarios Finales en el Ecosistema móvil. Los Activos de los Usuarios Finales son entre otros, los ETM conectados, los servicios, las aplicaciones, los sistemas de comunicaciones, y la totalidad de la información transmitida y/o almacenada en el Ecosistema móvil.[15]

XI. **Datos o Información personal:** Cualquier información concerniente a una persona física identificada o identificable.[16]

XII. **Desarrolladores de aplicaciones móviles**: Entidades que desarrollan aplicaciones móviles que estarán disponibles para los Usuarios Finales, a través de las Tiendas de aplicaciones y/o a través de los Operadores.[17]

XIII. **Dispositivo o Equipo Terminal Móvil (ETM):** Equipo que utiliza el usuario para conectarse más allá del punto de conexión terminal de una red pública con el propósito de tener acceso y/o recibir uno o más servicios de telecomunicaciones móviles; el cual también puede ser un dispositivo de computación portátil con un factor de forma pequeño de manera que puede ser transportado fácilmente; además está diseñado para funcionar sin una conexión física (por ejemplo, transmitir o recibir información de forma inalámbrica); posee almacenamiento de

---

[9] Ídem

[10] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=90.html

[11] https://csrc.nist.gov/glossary/term/brute_force_password_attack

[12] https://csrc.nist.gov/glossary/term/passive_attack

[13] Adaptada de: https://www.itu.int/rec/T-REC-X.1213/recommendation.asp?lang=es&parent=T-REC-X.1213-201709-I

[14] https://csrc.nist.gov/glossary/term/bluetooth

[15] Adaptada de: https://www.itu.int/rec/T-REC-X.1205-200804-I/es

[16] http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

[17] Adaptada de: *CTIA. Today's Mobile Cybersecurity*

datos interna y removible o externo; incluye una fuente de energía autónoma; puede incluir capacidades de comunicación por voz, sensores integrados que permiten la captura de información y/o funciones integradas para sincronizar datos locales (en el ETM) con ubicaciones remotas.[18]

XIV. **Ecosistema móvil:** Es el conjunto indivisible de Activos y servicios ofrecidos, integrado entre otros, por los Usuarios Finales, Operadores, fabricantes de ETM, tiendas de aplicaciones, desarrolladores de aplicaciones, proveedores de SO móviles, proveedores de servicios para la infraestructura de telecomunicaciones, proveedores de servicios de valor agregado.[19]

XV. **Entorno de ejecución confiable (TEE):** Entorno resistente a la manipulación y que se ejecuta por separado del núcleo del sistema operativo móvil.[20]

XVI. ***Firmware***: Programas de *software* e información almacenados en el *hardware*, generalmente en memorias de solo lectura, a efecto de que los programas y la información no se puedan sobre escribir o modificar durante la ejecución de los programas.[21]

XVII. **Ingeniería social:** Técnicas, procedimientos y medios utilizados por los Atacantes aprovechando la confianza de los Usuarios Finales para conseguir, entre otros, información personal, contraseñas, y parámetros de conexión para suplantar su identidad, con el objeto de engañar a los sistemas y penetrar en éstos haciéndose pasar por las personas habilitadas.[22]

XVIII. **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.[23]

XIX. ***Jailbreaking* o *Rooting***: Proceso que aprovecha las vulnerabilidades de un ETM para instalar *software* distinto al que el fabricante ha puesto a disposición del propio ETM. El *Jailbreaking o Rooting* permite al propietario del ETM obtener acceso al núcleo del sistema operativo y a configuraciones restringidas a las que normalmente no podría aplicar o acceder.[24]

XX. ***Malware:*** *Software* malicioso diseñado específicamente para dañar o interrumpir un sistema; atacando su confidencialidad, integridad y disponibilidad.[25]

XXI. **Módulo de seguridad:** Conjunto de *hardware*, *software* y/o *firmware* que implementa las funciones de seguridad en un TEE.[26]

XXII. **Proveedores de servicios de soporte a la infraestructura de la Red Pública de Telecomunicaciones**: Entidades que prestan servicios a los operadores relacionados con la infraestructura Red Pública de Telecomunicaciones.[27]

---

[18] https://csrc.nist.gov/glossary?sortBy-lg=relevance&ipp-lg=100

[19] Adaptada de: https://www.gsma.com/latinamerica/wp-content/uploads/2016/09/ME_LATAM_2016-Spanish-Report-FINAL-Web-Singles-1.pdf

[20] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-21.pdf

[21] https://csrc.nist.gov/glossary/term/firmware

[22] Adaptada de: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2007-PDF-S.pdf

[23] *International Standard ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[24] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-21.pdf

[25] https://csrc.nist.gov/glossary/term/malware

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

[27] Adaptada de: *CTIA. Today's Mobile Cybersecurity*

XXIII. **Proveedores de servicios de valor agregado**: Entidades que brindan servicios complementarios a los Usuarios Finales a través de la Red Pública de Telecomunicaciones.[28]

XXIV. **Seguridad de la Información:** Protección contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados de la información y los sistemas de información, con el fin de brindar confidencialidad, integridad y disponibilidad de esta.[29]

XXV. **Superficie de ataque**: Conjunto de puntos en la frontera de un sistema, elemento del sistema o del entorno donde un Atacante puede intentar ingresar, provocar un efecto, daño o extraer información del sistema, del elemento del sistema o del entorno en mención.[30]

XXVI. **Tarjeta SIM:** Módulo de Identidad del Suscriptor (SIM, del inglés "*Subscriber Identity Module*"); tarjeta de circuito integrado que contiene información sobre el suscriptor relacionada con la red de telecomunicaciones.[31]

XXVII. **Usuario Final**: Persona física o moral que utiliza un servicio de telecomunicaciones como destinatario final.[32]

XXVIII. **Vulnerabilidades**: Fallas de seguridad que pueden traducirse, intencional o accidentalmente, en una violación de la política de seguridad.[33]

4. Abreviaturas

En el presente Código se emplean las siguientes abreviaturas:

API	Interfaz de Programación de Aplicaciones (del inglés, "*Application Programming Interface*").
CPU	Unidad Central de Procesamiento (del inglés, "*Central Processing Unit*").
DoS	Denegación de Servicio (del inglés, "*Denial of Service*").
DDoS	Denegación de Servicio Distribuida (del inglés, " *Distributed Denial of Service, "*).
eSIM	Módulo de Identidad del Suscriptor Integrado (del inglés, "*Subscriber Identity Module Embedded*").
GNSS	Sistema Global de Navegación por Satélite (del inglés "*Global Navigation Satellite System* ").
GSMA	Asociación del Sistema Móvil Global (del inglés, "*Global System Mobile Association").*
HSS	Servidor Domestico de Suscriptores (del inglés, "*Home Subscriber Server*").
IoT	Internet de las Cosas (del inglés, "*Internet of Things*").
IP	Protocolo de Internet (del inglés "*Internet Protocol*").
MMS	Servicio de Mensajes Multimedia (del inglés, "*Multimedia Message Service*").
M2M	Máquina a Máquina (del inglés, "*Machine to Machine*").
NFC	Comunicación de Campo Cercano (del inglés, "*Near Field Communication*").
NIP	Número de Identificación Personal (del inglés, "*Personal Identification Number*").

[28] Ídem
[29] https://csrc.nist.gov/glossary/term/infosec
[30] https://csrc.nist.gov/glossary/term/attack_surface
[31] http://www.ift.org.mx/sites/default/files/2018_07_30_mat_ift.pdf
[32] *Artículo 3, fracción LXXI de la LFTR*
[33] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2007-PDF-S.pdf

NIST	Instituto Nacional de Estándares y Tecnología (del inglés, "*National Institute of Standards and Technology*").
SD	Seguridad Digital (del inglés, "*Secure Digital*").
SDHC	SD de Alta Capacidad (del inglés, "*Secure Digital High Capacity*").
SDIO	SD Entrada/Salida (del inglés, "*Secure Digital Input/Output*").
SDSC	SD de Capacidad Estándar (del inglés, "*Secure Digital Standard Capacity*").
SDUC	SD Ultracapacidad (del inglés, "*Secure Digital Ultra Capacity*").
SDXC	SD Capacidad Extendida (del inglés, "*Secure Digital Extended Capacity*").
SMS	Servicio de Mensajes Cortos (del inglés, "*Short Message Service*").
SO	Sistema Operativo (del inglés, "*Operating System*").
SoC	Sistema en Circuito Integrado (del inglés, "*System on a Chip*").
RoT	Raíz de la Confianza (del inglés, "*Roots of Trust*").
RTOS	Sistema Operativo en Tiempo Real (del inglés, "*Real Time Operating System*").
TEE	Entorno de Ejecución Confiable (del inglés, "*Trusted Execution Environment*").
UICC	Tarjeta de Circuito Integrado Universal (del inglés, "*Universal Integrated Circuit Card*").
USB	Bus Serial Universal (del inglés, "*Universal Serial Bus*").
USIM	Módulo de Identidad de Suscriptor Universal (del inglés, "*Universal Subscriber Identity Module*").
Wi-Fi	Fidelidad Inalámbrica (del inglés, "*Wireless Fidelity*").
3GPP	El Proyecto de Asociación de Tercera Generación (del inglés, "*The 3rd Generation Partnership Project*").

5. Panorama General de Amenazas del ETM

5.1 Ecosistema móvil

El Ecosistema móvil es un conjunto indivisible de Activos y servicios ofrecidos por diferentes entidades (descritas más adelante), en donde los ETM al hacer uso de la movilidad que les proporciona la conectividad ubicua, interactúan con redes de telecomunicaciones, sistemas de información y otros dispositivos interconectados entre sí.

La Asociación de fabricantes de Equipo Inalámbrico de los Estados Unidos de América (por sus siglas en inglés, *CTIA*), destacó en el documento *"Today's Mobile Cybersecurity, Blueprint for the Future"* la complejidad del Ecosistema móvil actual, así como los requerimientos de seguridad interdependientes entre un conjunto indivisible de Activos y servicios ofrecidos por las diferentes entidades.

A continuación, se enlistan de manera enunciativa, más no limitativa, las diversas entidades que forman parte del Ecosistema móvil:

I. Usuarios Finales;
II. Operadores;
III. Fabricantes de ETM;
IV. Tiendas de aplicaciones móviles;
V. Desarrolladores de aplicaciones móviles;
VI. Proveedores de SO móviles;
VII. Proveedores de servicios de valor agregado;
VIII. Fabricantes de microcircuitos;
IX. Fabricantes de equipos de la Red Pública de Telecomunicaciones, y
X. Proveedores de servicios de soporte a la infraestructura de la Red Pública de Telecomunicaciones (proveedores de *software* de red y servicios a los sistemas de red).

A continuación, la Figura 1, muestra algunas de las interacciones entre las diferentes entidades arriba listadas en el Ecosistema móvil.[34]

[34] https://api.ctia.org/docs/default-source/default-document-library/cybersecurity_white_paper.pdf

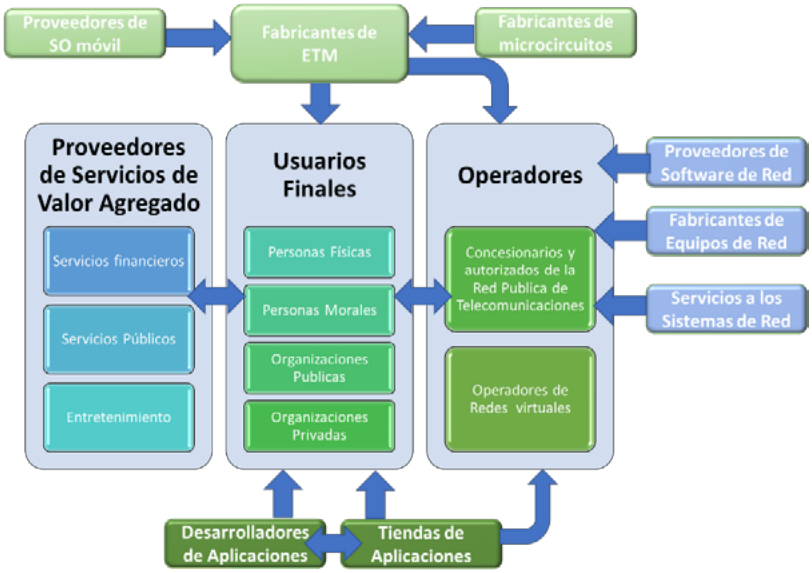

Figura 1. Entidades que conforman el Ecosistema móvil.

En sus inicios los ETM contaban con funciones básicas, diseñados principalmente para realizar llamadas de voz; así mismo fueron los Operadores el blanco de ataques, por quienes buscaban realizar llamadas de voz gratuitas, sin embargo, el panorama de Amenazas cambió, una vez que los ETM comenzaron a emplear SO móviles, los cuales han brindado desde su aparición más funcionalidades y servicios; lo anterior derivó, en que los Usuarios Finales comenzaran a confiar su información personal a las aplicaciones móviles instaladas en el ETM propiciando la creación de Vulnerabilidades y Amenazas.[35]

La idea central es proteger los Activos y servicios que se llevan a cabo en el Ecosistema móvil, ya que no puede existir privacidad de la información sin seguridad. Por lo que, en este Código se identificarán y definirán las entidades o componentes que integran el Ecosistema móvil; así como, las características de seguridad, los estándares técnicos, los protocolos, el *hardware,* el *software,* que permiten en su conjunto disfrutar de los Activos y los servicios móviles dentro del referido ecosistema. Lo anterior, a efecto de mitigar las Amenazas, Vulnerabilidades, riesgos y ataques a la seguridad, de los que son objeto los ETM, así como la información en general contenida en éste.

Por otro lado, para entender las Amenazas, Vulnerabilidades, riesgos y ataques dentro del Ecosistema móvil a los que están expuestos los ETM, es relevante identificar las Superficies de ataque que podrían ser empleadas por los Atacantes para intentar ingresar, provocar daño o extraer información del sistema, del elemento del sistema o del entorno en mención al explotar las Vulnerabilidades de estos.

En ese orden de ideas, las posibles Superficies de ataque son:

a. El *hardware* integrado, entre otros, por los componentes de nivel inferior (el procesador principal, el de banda base y el de la Tarjeta SIM/UICC), así como la tarjeta de

[35] https://www.dhs.gov/publication/st-mobile-device-security-study

almacenamiento SD, el puerto de suministro eléctrico y sincronización, los Módulos de seguridad, periféricos, sensores, cámaras y micrófonos, etc.

b. El *software,* centrándose en aplicaciones móviles, SO móvil y *Firmware* del ETM.
c. Las redes de telecomunicaciones con las que interactúan los ETM, por ejemplo, la Red Pública de Telecomunicaciones, redes Wi-Fi, redes Bluetooth y NFC, entre otras.
d. Las relacionadas a los proveedores de servicios de valor agregado, que pueden incluir a las tiendas de aplicaciones móviles, servicios financieros, tiendas de descarga de contenido, así como, los servicios de respaldo proporcionados por el fabricante del ETM o el proveedor del SO móvil, por mencionar algunos y
e. El acceso físico al ETM, el cual se refiere a la pérdida o robo del ETM que pudiera derivar en el acceso a la Información Personal del Usuario Final.

5.2 Amenazas para el ETM

La Unión Internacional de Telecomunicaciones en su recomendación *"ITU-T X.1120-X.1139 Series, Supplement on security aspects of smartphones"*[36], establece que las Amenazas representan posibles violaciones a la seguridad en los ETM, y que pueden clasificarse en las siguientes categorías:

I. Vulnerabilidades y
II. Ataques.

Por lo que, las Vulnerabilidades son fallas de los sistemas o debilidades en los procedimientos de seguridad relativos a los controles internos o la implementación; por otro lado, los ataques son intentos para causar daños intencionales, realizar accesos no autorizados o modificaciones maliciosas en los ETM. En otras palabras, las Vulnerabilidades están relacionadas con las características internas de los ETM mientras que los ataques son las actividades ofensivas externas a éstos.

La mayoría de los intentos por explotar las Vulnerabilidades en los ETM tiene como objeto iniciar un ataque. Por ejemplo, un *Malware* instalado pudiera eliminar ciertos archivos almacenados en un ETM sin que el Usuario Final este enterado. En este ejemplo, el *Malware* es el ataque, mientras que la falta del conocimiento de ataque al Usuario Final es la Vulnerabilidad.[37]

5.2.1 Clasificación de las Vulnerabilidades

Los ETM pueden contener numerosas Vulnerabilidades tales como:

[36] https://www.itu.int/rec/T-REC-X.Sup19/en
[37] Ídem

I. **Fallas del sistema**: Es preciso señalar que por diseño se busca prevenir todas las falla en *hardware* y *software*, sin embargo, algunas fallas pueden observarse desde etapas iniciales, y otras permanecen ocultas o latentes hasta que son explotadas. Incluso cuando se detectan algunas fallas principalmente en *hardware* estas son difíciles de solucionar.

II. **Gestión insuficiente de API**: Se refiere al proceso de desarrollo, publicación y administración de las API. Generalmente, las API de los ETM se clasifican en API controladas para gestión remota y API abiertas para aplicaciones de terceros. Estas primeras generalmente cuentan con usuarios o perfiles de administrador que les brindan privilegios para realizar actualizaciones remotas de las aplicaciones y del SO móvil, eliminación de archivos y recuperación de información; sin embargo, una gestión no adecuada o insuficiente de estos usuarios o perfiles, puede derivar en actividades maliciosas que conllevan a ataques de puerta trasera. Por otro lado, las API abiertas al ser del dominio público, sin ningún responsable de su gestión, corren un mayor riesgo de ser utilizadas para iniciar ataques.

III. **Falta de conocimiento del Usuario Final**: Algunas aplicaciones móviles pueden instalarse en los ETM sin el consentimiento o confirmación o con información limitada para el Usuario Final; lo anterior, es aprovechado por los Atacantes para distribuir aplicaciones móviles que contienen *Malware*, las cuales posteriormente realizarán operaciones sin el conocimiento del Usuario Final, como es el envío y recepción de mensajes, eliminación de archivos importantes, y/o activación de interfaces periféricas en el ETM, entre otras. Por lo que, los Usuarios Finales solo se percatarán de estos ataques, cuando la ejecución de dichas actividades propicie incidentes graves no deseados.

IV. **Canales de comunicaciones inseguros**: En entornos inalámbricos (Redes Públicas de Telecomunicaciones, redes Wi-Fi, NFC y Bluetooth) la información del Usuario Final y de las señales de control transmitidas entre el ETM y los dispositivos de la red pueden ser interceptadas a medida que se transmiten por la interfaz aérea. Derivado de lo anterior, si estos canales de comunicaciones no son protegidos, es decir, no se emplea un proceso de cifrado extremo a extremo, la información del Usuario Final quedará expuesta. Es relevante mencionar, que la mayoría de los canales inalámbricos no cuentan con suficientes mecanismos de protección de seguridad debido a las siguientes razones:

   a. Seguridad deficiente o insuficiente en los protocolos de comunicación utilizados en los canales inalámbricos, y
   b. Consideraciones relativas a los altos costos de implementación de soluciones de seguridad.

5.2.2 Clasificación de Ataques

Como se ha mencionado, los ETM contienen Activos valiosos para los Atacantes tales como *software*, *hardware* e Información Personal, en especial aquella relacionada con los sistemas financieros. A efecto de obtener dicha información los Atacantes podrían llevar a cabo algunos de los siguientes ataques:

I. **Ataques de acceso físico**: El tamaño y forma de los ETM permite al Usuario Final una fácil transportación y manejo, lo que los hace más propensos a ser robados o extraviados. En ese sentido, sin las medidas de protección adecuadas, la información personal del Usuario Final almacenada en los ETM, como son, la información relativa al sistema financiero, a las contraseñas de las cuentas de correo electrónico, a las redes sociales, los mensajes de texto, los registros de comunicación, etc., podrá leerse directamente en el ETM. Adicionalmente, en el caso, de reemplazo del ETM por daño o de sustitución por varios años de uso, la eliminación incorrecta de la información puede incrementar el riesgo ya que mediante el uso de algún *software* de reciclaje los Atacantes podrían recuperar dicha información confidencial la cual fue borrada superficialmente del ETM.

II. **Ataques con *Malware***: El *Malware* puede propagarse al descargar una aplicación móvil de la cual el Usuario Final desconoce su funcionamiento; incluso si las aplicaciones móviles cuentan con el consentimiento explícito del Usuario Final, estas pueden actuar de forma maliciosa sin que los Usuarios Finales se percaten de este hecho. Las formas más frecuentes de propagar *Malware* son:

   a. Descarga de archivos infectados desde Internet.
   b. Repositorios en línea de aplicaciones móviles.
   c. Servicios de mensajería.
   d. Comunicaciones vía Bluetooth y
   e. Comunicaciones vía NFC.

   Por otro lado, el *Malware* puede comportarse de distintas maneras y sus consecuencias posteriores son amplias; éste, también puede emplearse para intentar propagarlo a otros dispositivos portátiles o incluso a computadoras personales para ampliar su efecto, o en su caso, afectar a toda la red de comunicaciones. En ese sentido, a continuación, se muestran algunos Ataques que hacen usos del *Malware* y de otras estrategias:

   i. **DoS:** Es un ataque que produce una denegación o degradación de la calidad del servicio móvil cuando los Atacantes sobrecargan las redes del servicio móvil con tráfico falso, empleando *Botnets* o mediante el robo del servicio prestado a los Usuarios Finales. Lo anterior, produce que el servicio o recurso resulte inaccesible, derivado de la pérdida de la conectividad por una alta demanda y/o consumo total del ancho de banda que brinda el servicio a los Usuarios Finales.
   ii. **Geolocalización:** Este ataque consiste en realizar un seguimiento del desplazamiento físico del Usuario Final; lo anterior, mediante la obtención pasiva o activa de las coordenadas geográficas tridimensionales del ETM, con la que se puede obtener información de la velocidad y dirección del ETM en posesión del Usuario Final.
   iii. **Divulgación de información:** Se refiere a la intercepción, filtración o extracción de información en tránsito de las aplicaciones móviles instaladas en el ETM que pueden derivar en Ataques Pasivos o Activos.
   iv. ***Phishing***. Es un ataque que mediante la Ingeniería social tiene como objeto adquirir de manera fraudulenta información personal de los Usuarios Finales (principalmente

información de los servicios financieros). Los Atacantes emplean el *Spam* para alcanzar el mayor número posible de víctimas e incrementar sus posibilidades de éxito. Una vez que el *Spam* es entregado al destinatario, éste mediante engaños intenta persuadir a los Usuarios Finales para que proporcione información personal; o también, lo conduce a sitios de Internet, aparentemente de sitios oficiales con *Malware* en donde los Atacantes terminan de persuadir al usuario a que introduzca información personal (número de cuenta, contraseña, número de seguridad social, etc.) relativos a servicios financieros.[38]

v. ***Tampering***: Es un ataque que modifica un sistema, los componentes de éste o sus datos de forma no autorizada, con el objetivo de afectar su comportamiento esperado. Algunos ejemplos de estos son la modificación de la información en tránsito; insertar *hardware* y/o *software* alterado en la cadena de suministro del ETM; empaquetar *Malware* en aplicaciones móviles legítimas; o modificar la configuración de la Red Pública de Telecomunicaciones que emplea el ETM.

III. **Ataques de puerta trasera:** Se generan principalmente por errores en la divulgación de las API controladas y por la explotación de Vulnerabilidades de seguridad en algunos SO móviles, tales como autenticaciones insuficientes y autorizaciones incorrectas. Aunado a lo anterior, si los Atacantes conocen el funcionamiento de las API, éstos pueden actuar como entidades legítimas en los ETM. Con base en estas Vulnerabilidades, los Atacantes pueden eludir las políticas de seguridad de acceso a los ETM e iniciar algún ataque.

IV. **Ataques a redes de telecomunicaciones:** Derivado de las múltiples interfaces de conexión con que cuentan los ETM (Red Pública de telecomunicaciones, Wi-Fi, Bluetooth, NFC y GNSS) para acceder a los servicios de valor agregado, éstos son susceptibles a Ataques pasivos (por ejemplo, escucha de comunicaciones, captura y análisis de información en tránsito, Geolocalización y Divulgación de información) y Ataques Activos (por ejemplo, suplantación de identidad, corrupción, bloqueo o modificación de información).

Nota: Generalmente, los Ataques pasivos son empleados como plataforma por los Ataques Activos a efecto de recopilar información de los objetivos del ataque.

V. **Ataque de Clonación**: La información de la autenticación, claves y algoritmos criptográficos son almacenadas en el ETM o en la Tarjeta SIM/UICC y proporcionan los mecanismos para comprobar la identidad de un usuario que pretende iniciar sesión en la Red Pública de Telecomunicaciones móvil; estos mecanismos proporcionan los medios para evitar exponer la información de autenticación y que esta sea clonada.

VI. **Ataques a la interfaz periféricas:** Los ETM regularmente cuentan con distintas interfaces periféricas, como el puerto USB (empleado algunas veces como puerto de suministro eléctrico y sincronización) y las interfaces de conexión a la Red Pública de telecomunicaciones, Wi-Fi, Bluetooth, NFC, GNSS, entre otros; las cuales incrementan la capacidad de comunicación del ETM, pero al mismo tiempo incrementan las Superficies de ataque. Los Atacantes pueden instalar *Malware* en el ETM utilizando por ejemplo el puerto de suministro eléctrico y

[38] https://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

sincronización; por otro lado, mediante la activación de las interfaces periféricas (cámaras y micrófonos) los Atacantes podrían recolectar y transferir Información confidencial del Usuario Final.

VII. **Acceso no autorizado**: Los mecanismos de autenticación pudieran contener Vulnerabilidades que pueden explotarse, ya que algunas medidas de seguridad no son lo suficientemente robustas contra los Ataques de diccionario; otros mecanismos de autenticación cuentan con puertas traseras integradas y diseñados por los propios fabricantes de ETM para eludir todo o parte del mecanismo de seguridad.

VIII. ***Spam***: Son mensajes en formatos SMS, MMS y correos electrónicos, entre otros, enviados de forma masiva a los ETM (conocidos también como "*mensajes basura*"), y que empleando técnicas de Ingeniería Social pretenden persuadir a los Usuarios Finales para que realicen llamadas o envíen mensajes de texto a números de servicios con cargo. El *Spam* también es empleado para realizar otros ataques, como el *Phishing*, o un ataque con *Malware* que se encuentra adjunto al mensaje.

5.3 *Hardware* y *software* del ETM

Los ETM son similares en su arquitectura lógica funcional a las computadoras de escritorio, por lo que comparten de alguna forma las mismas Amenazas, Vulnerabilidades, riesgos y ataques; por otro lado, además de las Amenazas propias de su naturaleza, los ETM al incluir un estado permanente de operación, conectividad ubicua brindada por medio de múltiples interfaces de conexión como la interface a la Red Pública de telecomunicaciones, Wi-Fi, Bluetooth, y NFC; así como, una amplia variedad de sensores biométricos, y funcionalidades tales como GNSS, brújula, giroscopio, barómetro, cámaras y micrófonos, etc., los hace aún más susceptibles de ser blanco de ataques.

En la Figura 2 se ilustran, de forma enunciativa, mas no limitativa, las distintas interfaces de conexión y periféricas que pudiera contener un ETM.

Figura 2. Interfaces de Conexión y Periféricas en el ETM.

Estas características únicas de los ETM requieren comprender mejor el *hardware* y *software* que lo integran, ya que un análisis de ciberseguridad desde la óptica de una computadora de escritorio no es suficiente para el caso de los ETM.

En ese orden de ideas, en la Figura 3 se muestran de manera detallada las diferentes capas tecnológicas que integran a los ETM como son el *hardware* y el *software* (aplicaciones móviles, SO móviles y *Firmware*):

I. Capa de *hardware* del ETM, integrado por los componentes de nivel inferior, además de la tarjeta de almacenamiento SD, puerto de suministro eléctrico y sincronización, los Módulos de seguridad, periféricos, sensores, cámaras y micrófonos, entre otros.

II. Capa de *Firmware*, la cual integra los códigos de inicialización de los gestores de arranque o inicio y a los controladores de las diferentes interfaces de conexión.

III. Capa de SO móvil, cuyos elementos pueden incluir, entre otros, a las API, a los entornos aislados de aplicaciones, a los servicios multimedia, así como las utilerías para aplicaciones móviles y

IV. Capa de aplicaciones móviles, la cual está conformada por aplicaciones desarrolladas para ETM que emplean SO móviles y que proporcionan herramientas, recursos, juegos, acceso a redes sociales o a casi cualquier elemento descargable que incorpora funcionalidades o características a los ETM.

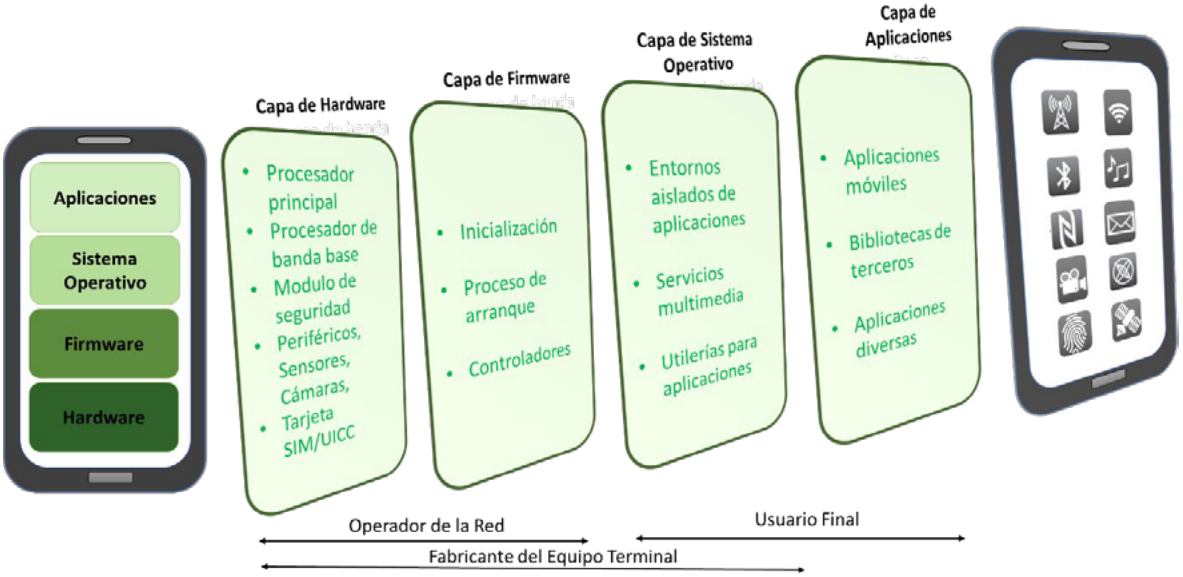

Figura 3. Capas tecnológicas de los ETM.

5.4 *Hardware*

5.4.1 Componentes de nivel inferior

Los componentes de nivel inferior son procesadores interdependientes integrados en el ETM, los cuales resultan imprescindibles para el funcionamiento seguro de éste.

El ETM contiene un procesador principal con su correspondiente gestor de arranque o de inicio (encargado de iniciar la ejecución del SO móvil) el cual, en caso de contener Vulnerabilidades o estar configurado de manera insegura, puede ser empleado por un Atacante para alterar o ejecutar una versión alterna del SO móvil, lo que pudiera dar como resultado un comportamiento malicioso en el ETM.

A su vez, el procesador principal cuenta con un TEE, que se ejecuta de manera independiente al SO móvil para brindar funcionalidades de seguridad, tales como el almacenamiento de información relacionada con los certificados digitales; el cifrado de la información y la verificación de la integridad del ETM, entre otros. La explotación de las Vulnerabilidades del procesador principal plantea un riesgo al ETM por que se pudiera vulnerar desde un inicio la seguridad.

Además del procesador principal, el ETM puede estar integrado por otros procesadores, como es el procesador de banda base que gestiona las conexiones inalámbricas (Red Pública de

Telecomunicaciones, Wi-Fi, Bluetooth y NFC) y el procesador de la Tarjeta SIM/UICC, el cual se describe con mayor detalle más adelante.

La Figura 4 muestra los procesadores interdependientes que pueden integrar al ETM.

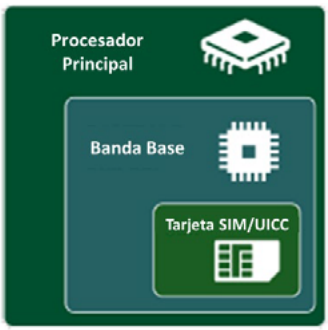

Figura 4. Procesadores independientes en el ETM.

5.4.2 Tarjeta SIM/UICC

Es una tarjeta de hardware extraíble conocida coloquialmente como Tarjeta SIM, sin embargo, las actuales generaciones de tarjetas SIM empleadas en ETM usan el término UICC, la cual es la base de la seguridad en las redes del servicio móvil. La Tarjeta SIM/UICC contiene un procesador integrado en un SoC que almacena la identidad del suscriptor móvil, las claves criptográficas previamente compartidas y la información de la configuración necesaria para obtener acceso a la red del servicio móvil.

La Tarjeta SIM/UICC ejecuta una aplicación de Java[39] denominada USIM, que es empleada para ejecutar un conjunto de funcionalidades que incluye entre otros, el proceso de autenticación del Usuario Final a la red del servicio móvil, el tipo de servicio contratado, la negociación de itinerancia internacional (Roaming), actualizaciones y los servicios basados en NFC. Las claves criptográficas son almacenadas en la Tarjeta SIM/UICC, la cual debe ser resistente a cualquier ataque de Tampering en el centro de autenticación del HSS (proceso que resulta crítico en la cadena de suministro, descrito más adelante).

Es importante mencionar que la Tarjeta SIM/UICC puede ser sustraída fácilmente de la mayoría de los ETM, por lo que ésta pudiera ser insertadas en cualquier otro ETM, con el objetivo de hacer uso de los servicios contratados y disponibles a través de la tarjeta sustraída.

[39] Fuente NIST: Es un lenguaje de programación desarrollado por Sun Microsystems. Java contiene una serie de características que lo hacen muy adecuado para su uso en el Internet. https://csrc.nist.gov/glossary/term/java

Por otro lado, la clonación de Tarjeta SIM/UICC, es un proceso que requiere acceso al repositorio de las claves criptográficas; sin embargo, mediante Ataques de Fuerza Bruta, que requieren equipo especializado, se pueden clonar tarjetas SIM/UICC en cuestión de horas.

La cadena de suministro relativa a la Tarjetas SIM/UICC se compone de al menos tres entidades distintas como se muestra en la Figura 5. Dichas tarjetas son fabricadas bajo las especificaciones proporcionadas por los Operadores, posteriormente son enviadas a un emisor de tarjetas y finalmente distribuidas en puntos de venta. Por lo que, en el referido proceso se puede comprometer la información contenida en la Tarjeta SIM/UICC.

Figura 5. Cadena de distribución de la Tarjeta SIM/UICC

En ese sentido, la seguridad de la cadena de suministro para las Tarjetas SIM/UICC se basa en la integridad de instalaciones seguras, la cual presenta diversos inconvenientes. A efecto de mitigar estos inconvenientes, la GSMA propuso una solución denominada eSIM que ofrece un nivel de protección y seguridad mejorada para los ETM. La solución eSIM extiende la seguridad de los ETM, al trasladar la seguridad basada en instalaciones físicas a una seguridad lógica presente en cualquier ubicación, donde el ETM se pueda acceder al HSS por medio de Internet.

Los mecanismos eSIM incorporan niveles superiores de seguridad e integridad en la transferencia de información. Asimismo, prevén un control sobre las conexiones de los ETM. Por lo que esta solución puede ser implementada bajo los siguientes modelos:

I. Solución para el Usuario Final: La característica principal de esta solución es que proporciona una interfaz para el Usuario Final, a efecto de que éste seleccione e interactúe con los servicios ofrecidos del Operador seleccionado, y

II. Solución M2M: Esta solución permite la gestión remota de perfiles de usuario, enfocados principalmente al suministro de tarjetas eSIM a las organizaciones; cabe señalar que la solución M2M difiere de la solución para el Usuario Final en cuanto a que no existe interacción con este último.[40]

***SIM Swap* o *SIM Swapping*:**[41] Es un tipo de fraude que inicia cuando los Atacantes toman el control del número telefónico del Usuario Final para acceder a sus llamadas y mensajes de texto, y posteriormente interceptar los mensajes de seguridad enviados por las entidades financieras, para finalmente tomar el control de las cuentas financieras de los Usuarios Finales.

Para efecto de lo anterior, los Atacantes recopilan Información Personal del Usuario Final que será utilizada para suplantar su identidad ante los Operadores, con el objetivo de iniciar el proceso de portabilidad numérica o en su caso obtener una nueva Tarjeta SIM/UICC que será insertada en otro ETM que posee y controla el Atacante. Otra forma es mediante la sustracción de la Tarjeta SIM/UICC del ETM del Usuario Final, la cual contiene un identificador único que almacena su Información Personal; con esto, el Atacante puede utilizar la Tarjeta SIM/UICC robada.[42]

Es preciso señalar que mediante técnicas de Ingeniería Social, los Atacantes pueden obtener Información Personal de los Usuarios Finales, como son, nombre, dirección, fecha de nacimiento y contraseñas; un ejemplo de cómo consiguen esto, es cuando los Atacantes realizan llamadas telefónicas a los Usuarios Finales, suplantando la identidad de una empresa o institución confiable, por lo general, la de una entidad financiera, la cual realiza diversas preguntas, con el objetivo de obtener la mayor cantidad de información personal posible.[43]

Finalmente, es importante mencionar que este tipo de fraudes son ataques pasivos, que no afectan en primera instancia a los ETM y sus componentes de *hardware* y *software*, así como a Redes Públicas de Telecomunicaciones y su infraestructura pasiva o activa.

5.4.3 Tarjeta de almacenamiento SD

Los ETM cuentan con los siguientes tipos de almacenamiento, empleados por las aplicaciones móviles instaladas en los ETM:

[40] https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf
[41] https://www.fcc.gov/sites/default/files/sim_swap_tip_card.pdf
[42] https://www.fcc.gov/consumers/guides/cell-phone-fraud
[43] https://www.fcc.gov/port-out-fraud-targets-your-private-accounts

I. Almacenamiento interno: Está conformado por hardware inmerso en el ETM y no se puede extraer físicamente. En este almacenamiento cada aplicación móvil guarda su propia información en una área privada, exclusiva y aislada de la información de otras aplicaciones.

II. Almacenamiento externo: Se realiza a través de una tarjeta de memoria externa que se inserta en el ETM y que es compartida por todas las aplicaciones móviles. Por ejemplo, para que una aplicación de mensajería pueda compartir o utilizar una foto de la galería de imágenes del ETM, la aplicación debe tener permisos para acceder a los archivos multimedia almacenados por una segunda aplicación en la tarjeta de almacenamiento externo.

Por lo anterior, para homogenizar el almacenamiento externo, en enero del año 2000, la Asociación SD desarrolló y promovió la adopción del estándar de tarjetas SD que son empleadas para almacenar cualquier tipo de información en los ETM. La Asociación SD incorporó *hardware* adicional a la tarjeta SD con el objeto de realizar el cifrado de la información que se resguarda en ésta.

El estándar de la tarjeta SD establece diferentes formatos de rendimiento, las cuales se utilizan regularmente para ampliar la capacidad de memoria o almacenamiento de los ETM. Las diferentes versiones de la tarjeta SD están diseñadas para optimizar el rendimiento de éstas y cumplir con los estándares SDSC / SDHC / SDXC / SDIO / SDUC. Además, las tarjetas SD se fabrican en los siguientes formatos: original SD, mini SD y micro SD; éste último, es el formato más utilizado en los ETM, el cual es compatible con la gran mayoría de ETM, lo que facilita el intercambio de información; sin embargo, también incorpora una Superficie de ataque.

En ese orden de ideas, se han documentado Vulnerabilidades y ataques a los tipos de almacenamiento que emplean los ETM; un ejemplo de esto se presenta cuando se descargan aplicaciones móviles, las cuales, posterior a su instalación son actualizadas con una versión que contiene *Malware*, o aplicaciones móviles que no observan las mejores prácticas en diseño de codificación segura. Estas últimas favorecen el uso del almacenamiento externo, ya sea, por la falta de espacio en el almacenamiento interno o para simular que requieren un menor espacio para ocultar sus deficiencias de seguridad.[44]

5.4.4 Puerto de suministro eléctrico y sincronización

El puerto de suministro eléctrico y sincronización es una interfaz periférica utilizada para proporcionar energía eléctrica a la batería del ETM, así como para habilitar la comunicación de dos vías para el respaldo e intercambio de la información con otros dispositivos. Esta interfaz puede estar disponible bajo alguno de los siguientes estándares:

I. USB tipo C;

[44] https://blog.checkpoint.com/2018/08/12/man-in-the-disk-a-new-attack-surface-for-android-apps/

II. Micro USB y
III. Propietarios y/o patentados por algunos fabricantes de ETM.

Derivado de lo anterior, los distintos casos de uso de la referida interfaz pueden generar Amenazas, Vulnerabilidades, riesgos y posibles ataques, cuando un ETM es conectado a una computadora o a una estación de carga no confiable. Lo anterior, permitiría a un Atacante utilizar el canal de comunicación para explotar Vulnerabilidades en el ETM y sustraer información de éste; se han documentado ataques de *Malware* y robo de información al conectar ETM a estaciones de carga públicas.[45]

Aunado a lo anterior, el puerto de carga y sincronización podría emplearse en el sentido inverso, es decir, cuando un ETM es utilizado para propagar *Malware,* al ejecutar ataques en contra del sistema de información o del dispositivo al que se conecta; un ejemplo de lo anterior, se presentó en ataques a los puertos de carga de las cabinas de aviones[46].

5.5 Software

5.5.1 Aplicaciones móviles

Una aplicación móvil es un programa diseñado para realizar funciones y tareas específicas que facilitan las actividades del Usuario Final; dichas aplicaciones permiten a éstos acceder a múltiples sensores integrados en el ETM, almacenar archivos, leer y escribir información y comunicarse con sitios de Internet para obtener acceso a diversos servicios e interactuar con otros Usuarios Finales.

La mayoría de las aplicaciones móviles son instaladas directamente en los ETM antes de ser comercializados o se encuentran disponibles a través de tiendas de aplicaciones, las cuales generalmente pertenecen a los desarrolladores de los SO móviles. Sin embargo, algunas organizaciones también distribuyen sus propias aplicaciones a través de tiendas privadas; estas aplicaciones no están pensadas para su distribución pública, sino para el uso al interior de la organización.

A continuación, la Figura 6 ilustra las Amenazas, Vulnerabilidades, riesgos y ataques más comunes a los ETM a través de aplicaciones móviles:

[45] https://usa.kaspersky.com/blog/usb-battery-charging-unsecurity/7195/
[46] https://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS

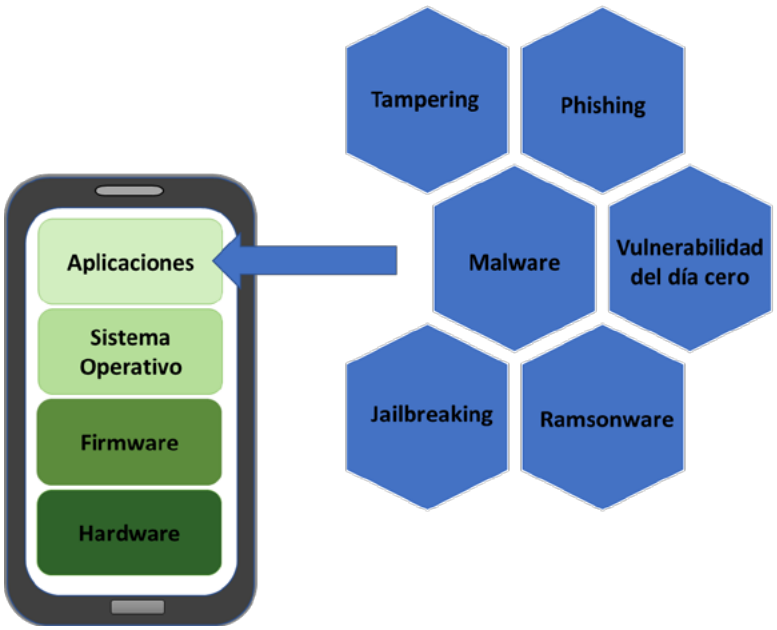

Figura 6. Amenazas, Vulnerabilidades, riesgos y ataques dentro para el ETM vía aplicaciones móviles.

Es importante mencionar, que en las aplicaciones móviles se presentan Vulnerabilidades que frecuentemente son el resultado de errores del desarrollador (programación) que no implementa mejores prácticas en materia de desarrollo de *software* (codificación segura). Cabe señalar, que la mayoría de las Vulnerabilidades en las aplicaciones móviles pueden ser detectadas durante la etapa de diseño mediante la revisión del código de programación; sin embargo, algunas Vulnerabilidades no son detectadas sino hasta que las aplicaciones están disponibles en las tiendas o en uso por los Usuarios Finales.

Aunado a lo anterior, las aplicaciones móviles pueden presentar otras Vulnerabilidades tales como:

I. **Conexión insegura.** Cuando una aplicación móvil requiere conectarse con un servidor remoto y se lleva a cabo sin el empleo de un mecanismo de cifrado extremo a extremo; lo anterior, habilita a un Atacante a interceptar dicha conexión y obtener Información Personal del Usuario Final. Así mismo, empleando la misma conexión, el Atacante puede realizar ataques de Hombre en el Medio (del inglés, "*Man-in-the-Middle*"), mismos que habilitan la escucha de comunicaciones privadas, o la modificación de la información a medida que esta es transmitida por la red de telecomunicaciones.

II. **Archivos almacenados en localidades de memoria inseguras o no protegidas.** Estas Vulnerabilidades se presentan cuando las aplicaciones móviles almacenan Información Personal del Usuario Final en un formato de texto plano en localidades de memoria inseguras o no protegidas.

III. **Información confidencial almacenada en la bitácora del sistema.** La bitácora del sistema contiene registros de las actividades y eventos del SO móvil, que documentan cómo se ejecutaron los procesos del sistema; sin embargo, algunas aplicaciones móviles que no siguen

las recomendaciones de la codificación segura, llegan a almacenar archivos en texto plano en la bitácora en comento, lo que facilita a los Atacantes obtener acceso a esta información.

IV. **Fallas en las medidas de seguridad del Navegador de Internet.** Este tipo de Vulnerabilidades se presenta en algunos navegadores de Internet instalados de forma predeterminada en los ETM, que generalmente son desarrollados sin observar recomendaciones de codificación segura y que son el punto de entrada a los ETM.

V. **Bibliotecas de terceros.** Los componentes o módulos de *software* de terceros empleados frecuentemente por los desarrolladores de aplicaciones móviles pueden llegan a contener Vulnerabilidades que, en su caso, pueden replicarse a cualquier aplicación móvil que haga uso de éstas, lo que eventualmente puede afectar a miles de Usuarios Finales. Por ejemplo, en el año 2015, se presentó una Vulnerabilidad en una biblioteca terceros que provocó que una aplicación móvil al momento de intentar establecer una conexión segura entre la aplicación móvil y los servicios Web deshabilitará la validación de certificados digitales, lo que permitió ataques de Hombre en el medio. Esta Vulnerabilidad en su momento afectó a una versión específica de la referida biblioteca la cual fue corregida rápidamente; sin embargo, seis meses después del descubrimiento de la Vulnerabilidad en comento, aproximadamente 1,000 aplicaciones móviles seguían siendo vulnerables, debido a las fallas en el proceso de parche de la aplicación.

VI. **Mecanismos Criptográficos.** Las Vulnerabilidades en las aplicaciones móviles instaladas en los ETM relativas al cifrado de la información se presentan cuando:

a. No existe un mecanismo de protección para la Información Personal del Usuario Final;
b. Cuando el algoritmo de cifrado implementado no es el adecuado y
c. No se emplean técnicas de cifrado recomendadas y validadas por instituciones internacionales (por ejemplo, las de NIST).

No obstante, las Vulnerabilidades arriba señaladas, es importante indicar que la arquitectura de los ETM está diseñada para coadyuvar a mitigar Vulnerabilidades presentes en las aplicaciones móviles, al prevenir interacciones no deseadas, entre estas.

5.5.2 Sistema Operativo Móvil

El SO móvil es el *software* encargado de administrar los recursos del ETM, así como de la operación adecuada del *hardware* y de las aplicaciones móviles instaladas en los ETM; brinda a los Usuarios Finales distintas funcionalidades, a través de interfaces periféricas tales como: sensores biométricos, GNSS, brújula, giroscopio, barómetro, cámaras y micrófonos, etc., así como a través de múltiples interfaces de conexión a la Red Pública de telecomunicaciones, Wi-Fi, Bluetooth, y NFC, entre otras.

El diseño de la arquitectura de seguridad de los SO móviles desempeña un papel importante en la protección del ETM contra de la explotación de Amenazas, Vulnerabilidades, riesgos y ataques, a

través de la capacidad de aislamiento de las diferentes aplicaciones; el SO móvil brinda protección contra comportamientos maliciosos controlando las interacciones permitidas entre el *hardware* y las aplicaciones móviles instaladas en el ETM.

En algunos SO móviles, las aplicaciones móviles no pueden acceder a los datos o a información almacenada por otras aplicaciones, lo que coadyuva a evitar que dichas aplicaciones interfieran con el comportamiento de otra aplicación. La capacidad de aislamiento entre aplicaciones móviles propicia que incluso, si se llegará a instalar *Malware* en el ETM, éste no podría sustraer o alterar información de otras aplicaciones.

Aunado a lo anterior, la capacidad de gestión brindada por el SO móvil al Usuario Final favorece el control sobre la instalación de aplicaciones móviles, mediante la selección de fuentes legítimas autorizadas.

Como con cualquier otro *software*, las Vulnerabilidades del SO móvil son descubiertas constantemente. Por lo general, cuando una nueva Vulnerabilidad es descubierta, es notificada inmediatamente a los desarrolladores del SO móvil quienes deben proporcionar una solución e incluirla en la siguiente actualización del SO móvil, conocido comúnmente como "*parche*". No obstante, es importante mencionar que existen Vulnerabilidades desconocidas por los desarrolladores del SO móvil; por lo tanto, no han sido corregidas y en consecuencia pudieran ser explotadas por los Atacantes; a este tipo de Vulnerabilidades se le conoce como *"vulnerabilidad de día cero"*.

Además, como se mencionó en secciones previas, si el gestor de arranque o inicio del SO móvil contiene Vulnerabilidades o está configurado de manera insegura, un Atacante podría alterar el código del SO móvil y cargar una versión alterna con un comportamiento malicioso; ejemplo de lo anterior, surge cuando los Usuarios Finales realizan el *Jailbreaking o Rooting* en el ETM, a efecto de habilitar capacidades que de otro modo no estarían disponibles en el ETM, lo que coloca a éste último en un estado inseguro, que puede ser explotado por los Atacantes.

5.5.3 Firmware

El *Firmware* es una de las capas tecnológicas de nivel inferior o subyacente en la arquitectura lógica funcional de los ETM (Ver figura 3), que interactúa estrechamente con la capa tecnológica del *hardware* para proporcionar servicios y funcionalidades al SO móvil y a las aplicaciones móviles (capas tecnológicas de niveles superiores) instaladas en el ETM.[47]

[47] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

En ese sentido, las capas tecnológicas de niveles superiores deben confiar inherentemente en las capas inferiores, lo que propicia una cadena de confianza entre capas tecnológicas que comúnmente se conoce como raíz o base de la confianza (RoT).[48]

Considerando lo anterior, es fundamental, que el *Firmware* y su información de configuración, generen una RoT, a efecto de preservar la confidencialidad, integridad y disponibilidad de la información en el ETM, ya que, un ataque exitoso al *Firmware* podría facilitar la instalación de *Malware* que modificaría los servicios que son proporcionados al *hardware,* provocando interrupciones a las operaciones o incluso dejar sin funcionamiento al ETM; otra consecuencia es que el Atacante tendría acceso a la información almacenada en el referido ETM.

En ese sentido, a continuación, se enuncian tres principios que coadyuvan a la resiliencia del *Firmware* de los ETM:

I. **Protección:** Mecanismos que coadyuvan a que el *Firmware* del ETM permanezca en un estado de integridad y protección contra ataques de *Tampering* y accesos no autorizados.

II. **Detección:** Mecanismos que permitan la detección, en cualquier momento, de algún daño en el *Firmware* del ETM y

III. **Recuperación:** Mecanismos que permitan la restauración del *Firmware* a un estado integral conocido; lo anterior, en caso de haber sufrido daño o un ataque exitoso de *Tampering*.

[48] https://csrc.nist.gov/csrc/media/events/ispab-february-2012-meeting/documents/feb1_mobility-roots-of-trust_regenscheid.pdf

6. Recomendaciones y Mejores Practicas

A continuación, se describen las recomendaciones de mejores prácticas enfocadas principalmente a las Superficies de ataque de *hardware* y *software*. Asimismo, se incluyen algunas otras recomendaciones aplicables a otras superficies, que podrán ser observadas por los fabricantes de ETM, las personas físicas o morales que desarrollen y proporcionen servicios y aplicaciones para los ETM, los Operadores y por los Usuarios Finales.

6.1 Sobre el uso y la operación del ETM.

El Usuario Final podrá elegir ETM cuyos fabricantes de ETM empleen el enfoque de seguridad por diseño, que cuenten con capacidades de arranque seguro y otras características de seguridad importantes, como las que describen más adelante. Adicionalmente, los fabricantes de ETM y Operadores a través de una política de divulgación, establecerán de manera anticipada el período de vida útil del ETM en la que se indique de manera explícita la duración del período mínimo de soporte de las actualizaciones de seguridad.

6.1.1 Activar el bloqueo de pantalla y contraseña de desbloqueo

Los Usuarios Finales procurarán activar la funcionalidad de bloqueo automático de pantalla en los ETM; la cual entrará en funcionamiento después de un período de inactividad previamente seleccionado; para el desbloqueo del ETM se requerirá introducir un NIP o contraseña.

6.1.2 Evitar acceder a los enlaces electrónicos

Los Usuarios Finales buscarán evitar hacer "clic" en enlaces electrónicos de remitentes no confiables recibidos mediante SMS, MMS y correos electrónicos ya que pueden redirigir a páginas de Internet con Malware.

6.1.3 Utilizar Software de seguridad

Los Usuarios Finales procurarán instalar *software* de protección de seguridad en el ETM que coadyuvará a detectar y mitigar posibles amenazas y/o vulnerabilidades en este, así como en las aplicaciones móviles. Si el ETM carece de éste, deberá recomendar al Usuario Final su instalación. Si el ETM cuenta con el s*oftware* de protección de seguridad instalado, éste podrá recomendar al Usuario Final la inspección periódica del SO móvil, así como su propia actualización[49].

[49] https://www.itu.int/rec/T-REC-X.1213/recommendation.asp?lang=es&parent=T-REC-X.1213-201709-I

6.1.4 Instalar los parches de seguridad

Los Usuarios Finales coadyuvarán a que sus ETM se mantengan actualizados instalando los últimos parches de seguridad a efecto de evitar la explotación de Vulnerabilidades conocidas públicamente.

6.1.5 Identificar la red Wi-Fi

Los Usuarios Finales procurarán evitar el uso de redes Wi-Fi y puntos de acceso públicos no confiables; de no ser posible lo anterior, el ETM, podrá habilitar de manera automática y durante la trasmisión, el cifrado extremo-extremo.[50]

6.1.6 Evitar la exposición del número telefónico

Los Usuarios Finales, evitarán la exposición pública de su número telefónico móvil en sitios de Internet; lo anterior, con el objeto de no exponer Información Personal, que en su caso, podría ser empleada en Ataques Pasivos o Activos.

6.1.7 Evitar modificar la configuración del ETM para la explotación de Vulnerabilidades

Los Usuarios Finales procurarán evitar el *Jailbreaking* o *Rooting* en sus ETM, a efecto de mitigar la instalación de *Malware* o explotación de Vulnerabilidades que se derivan de la habilitación de características restringidas en el SO móvil.

6.1.8 Utilizar cables que permiten solamente el suministro eléctrico

Los Usuarios Finales evitarán conectar ETM directamente en puertos USB para suministro eléctrico públicos, a menos que se emplee un cable o adaptador exclusivo de suministro eléctrico.[51]

6.1.9 Usar tarjetas de almacenamiento SD originales y formateadas

Los Usuarios Finales buscarán utilizar tarjetas de almacenamiento SD previamente formateadas mediante el menú de configuración del ETM. Lo anterior con el objeto de prevenir la instalación, de *Malware* que aproveche Vulnerabilidades existentes en los ETM.[52]

---

[50] https://www.itu.int/rec/T-REC-X.1213/recommendation.asp?lang=es&parent=T-REC-X.1213-201709-I
[51] https://www.dhs.gov/publication/st-mobile-device-security-study
[52] https://www.sdcard.org/downloads/formatter/

6.1.10 Sobre el IMEI

Los Usuarios Finales buscarán conocer el identificador IMEI de su ETM. El IMEI del ETM resulta vital en caso de robo o extravío para solicitar el bloqueo del servicio de manera inmediata al Operador.[53]

NOTA: Cada ETM tiene asignado en forma única de manera física y/o electrónica el código pregrabado del IMEI, que permita su identificación inequívoca. Dicho IMEI debe estar impreso en una etiqueta adherida, grabado físicamente en el ETM o almacenado de manera electrónica en el software del referido equipo; en este último caso, debe encontrarse disponible en la pantalla del ETM a través de la marcación electrónica * # 0 6 # (asterisco, numeral, cero, seis, numeral).

6.2 Sobre las contraseñas

6.2.1 Contraseñas únicas en ETM

En cualquier estado que no sea el predeterminado de fábrica las contraseñas para los ETM, deberán ser únicas o definidas por el Usuario Final. [54]

6.2.2 Mecanismos de Autenticación

Los fabricantes de ETM procurarán implementar mecanismos biométricos de autenticación (huella digital, reconocimiento facial, etc.) que consideren lo siguiente:

I. Emplear mecanismos de cifrado de la información, conforme a las propiedades de las aplicaciones móviles y de la tecnología;
II. Hacer uso de TEE para almacenar las claves de acceso.[55]

6.2.3 Uso de contraseñas en los ETM para proteger la Tarjeta SIM/UICC

Los Operadores procurarán implementar mecanismos de autenticación para proteger la Tarjeta SIM/UICC mediante el uso de contraseñas en los ETM, con el objeto de proteger a los Usuarios Finales en cada intercambio o sustitución de la tarjeta en comento.[56]

NOTA: Habilitar la contraseña de la Tarjeta SIM/UICC coadyuva a mitigar los accesos no autorizados a la Red Pública de Telecomunicaciones en caso de pérdida o robo de esta o del ETM. En el supuesto anterior, en caso de sustituir la Tarjeta SIM/UICC en otro ETM, se deberá

[53] http://www.ift.org.mx/usuarios-y-audiencias/imei
[54] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf
[55] Ídem
[56] https://www.itu.int/en/publications/Documents/tsb/2019-Technical-report-on-SS7-vulnerabilities/index.html

ingresar la contraseña antes de continuar el registro del ETM en la red del servicio móvil. Muchas tarjetas SIM/UICC se bloquean después de tres intentos fallidos, por lo que el Operador podrá proporcionar un código de desbloqueo al Usuario Final para que dicha tarjeta sea utilizada nuevamente.

6.3 Sobre la gestión de informes de Vulnerabilidades

6.3.1 Información de contacto

Los fabricantes de ETM procurarán poner a disposición de sus Usuarios Finales una política de divulgación de Vulnerabilidades,[57] que al menos considere lo siguiente:

I. Información de contacto para la notificación de Vulnerabilidades, y
II. La información relativa a los plazos para:

   a. El acuse de notificación inicial de Vulnerabilidades, y
   b. La actualización del estatus de la Vulnerabilidad notificada hasta resolución de esta.[58]

6.3.2 Divulgación de Vulnerabilidades

Los fabricantes de ETM buscarán informar las Vulnerabilidades de seguridad directamente a las partes afectadas en primera instancia. Adicionalmente, fomentarán la cooperación y coordinación entre las partes interesadas, lo anterior para mitigar Amenazas, riesgos y ataques en el Ecosistema móvil.

6.4 Sobre el *software*

6.4.1 Aplicaciones móviles

El desarrollo e implementación de actualizaciones de seguridad para las aplicaciones móviles de forma oportuna es una de las acciones más importantes que los fabricantes de ETM pueden realizar para proteger a sus Usuarios Finales y al Ecosistema móvil. Las Vulnerabilidades a menudo provienen de componentes de aplicaciones móviles que no se prevé guarden relación

[57] Una política de divulgación de vulnerabilidades especifica claramente el proceso mediante el cual los investigadores en seguridad y otros grupos interesados puedan aportar información sobre las vulnerabilidades detectadas. Dicha política puede actualizarse conforme sea necesario para garantizar la transparencia y la claridad entre el fabricante de ETM y los investigadores de seguridad y viceversa.

[58] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

con la seguridad. Es una buena práctica que todo el *software* se mantenga actualizado y en buen estado. Lo anterior, con base en la política sobre el término de la vida útil de los ETM en la que se indique de manera explícita la duración mínima del período durante el cual dicho dispositivo recibirá actualizaciones de *software*, y el motivo de la duración del período de asistencia. Además, indicará claramente a los Usuarios Finales la razón por la que cada actualización es necesaria.[59]

6.4.2 Actualización segura

Los Usuarios Finales procurarán evitar la descarga de aplicaciones móviles de tiendas de aplicaciones no autorizadas.[60] Algunas tiendas oficiales de aplicaciones verifican que dichas aplicaciones no contengan *Malware*.[61]

6.4.3 Acceso a elementos del ETM

En caso de instalar aplicaciones móviles en el ETM, los Usuarios Finales procurarán verificar a qué elementos del ETM estas aplicaciones solicitan acceso; incluyendo el *software* de aplicaciones de navegadores de Internet, y aplicaciones en páginas de Internet;[62] por lo que, el funcionamiento del ETM estará bajo la observancia del *"principio de privilegio mínimo"*.[63]

6.4.4 Cifrar la Información Personal

Los EMT, así como las aplicaciones móviles instaladas en este podrán ofrecer al Usuario Final mecanismos para almacenar de forma cifrada la Información Personal que pudiera generarse o emplearse por éstas; por ejemplo, las listas de contactos, SMS, MMS, fotografías, registros de llamadas, etc.[64]

6.4.5 Alertar por vinculación de cuentas financieras

En su caso, el ETM o las aplicaciones móviles instaladas en este procurarán advertir al Usuario Final sobre el riesgo de guardar la información financiera o contraseñas empleadas en pagos de servicios en línea en el ETM.[65]

---

[59] https://www.dhs.gov/publication/st-mobile-device-security-study
[60] Ídem
[61] https://support.apple.com/es-mx/guide/security/sec35dd877d0/web
[62] https://www.dhs.gov/publication/st-mobile-device-security-study
[63] Este principio es la base de una buena ingeniería de seguridad, aplicable tanto a ETM como a cualquier otro campo
[64] https://www.itu.int/rec/T-REC-X.1213/recommendation.asp?lang=es&parent=T-REC-X.1213-201709-I
[65] Ídem

6.4.6 *Supervisar el rendimiento y consumo de datos en los ETM*

En su caso, el ETM o las aplicaciones móviles instaladas en este buscarán supervisar el rendimiento del CPU, del consumo de la batería y/o el consumo de datos, que permita determinar un consumo irregular, a efecto de enviar una alerta al Usuario Final informando de esta situación, la cual puede derivar en un posible ataque de *Malware*.[66]

6.4.7 *Usar mecanismos de verificación de terceros*

En su caso, las aplicaciones móviles instaladas en el ETM cuyo uso previsto incluya la realización de pagos de servicios en línea o cualquier otra operación financiera que requiera la identificación de la cuenta, podrán autenticar al Usuario Final mediante una aplicación de verificación de tercera parte pudiendo emplear mecanismos biométricos.[67]

Las aplicaciones de autenticación de tercera parte pueden emplearse para generar códigos de inicio de sesión que permitan confirmar la identidad por ejemplo al inicio de sesión por primera vez en un nuevo ETM.[68]

6.4.8 *Automatización de las actualizaciones*

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

6.4.9 *Divulgación de las actualizaciones*

Los fabricantes de ETM y los Operadores buscarán informar a los Usuarios Finales sobre el requerimiento de actualizaciones de aplicaciones móviles 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 y será de fácil implementación para los Usuarios Finales.[69]

6.4.10 *Eliminar Malware del ETM*

[66] https://www.itu.int/rec/T-REC-X.1213/recommendation.asp?lang=es&parent=T-REC-X.1213-201709-I
[67] Ídem
[68] https://es-la.facebook.com/help/358336074294704
[69] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf

En su caso, el *software* de protección de seguridad instalado en el ETM podrá detectar *Malware* e informar al Usuario Final de esta situación para que realice la acción correspondiente. En su caso, el referido *software* al detectar aplicaciones móviles con *Malware* y previa autorización del Usuario Final podrá informar a los fabricantes de ETM y a los Operadores con el objeto de integrar una posible *"lista negra"* de aplicaciones móviles que contengan *Malware*.[70]

6.4.11 Sobre el diseño de software para aplicaciones móviles

Los fabricantes de ETM, en las etapas de diseño y desarrollo del *software* de aplicaciones móviles, procurarán considerar hacer uso de mejores prácticas que se listan a continuación:[71]

I. Emplear estándares y mejores prácticas en materia de Ciberseguridad publicadas por los desarrolladores de SO móvil[72], [73].
II. Utilizar herramientas de detección o diagnóstico de Vulnerabilidades o riesgos antes de la implementación de dichas aplicaciones.
III. Aplicar métodos de Seguridad de la Información en las capas de red y transporte relativas al protocolo IP, con el objeto de proteger dichas aplicaciones de Amenazas, Vulnerabilidades, riesgos y ataques en la Red Pública de Telecomunicaciones.
IV. Hacer uso de kits de desarrollo de *software* que coadyuven al cifrado de la información para fortalecer el control de acceso, y la interacción controlada de la información entre distintas aplicaciones y
V. En su caso, los Operadores en un ambiente controlado podrán emplear herramientas comerciales de verificación de terceros para aplicaciones móviles a efecto de evaluar éstas en busca de Vulnerabilidades comunes.

6.4.12 Sobre el Sistema Operativo Móvil

Los Usuarios Finales procurarán ejecutar la última versión del SO móvil disponible para el ETM; la cual podrá incluir mejoras en el diseño de los mecanismos de seguridad del ETM, a efecto de mitigar Amenazas, Vulnerabilidades, riesgos y ataques a las aplicaciones móviles.

6.4.13 Habilitar una API en el SO móvil

Los Operadores procurarán agregar *software* (API) entre el SO móvil y el *Firmware* del ETM, que en su caso, permitirá a los éstos monitorear el estado de la interacción entre el ETM y la infraestructura de su red.[74]

---

[70] https://www.itu.int/rec/T-REC-X.1213/recommendation.asp?lang=es&parent=T-REC-X.1213-201709-I
[71] https://www.dhs.gov/publication/st-mobile-device-security-study
[72] https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide/Introduction.html
[73] https://developer.android.com/design-for-safety#security
[74] https://techcrunch.com/2011/12/01/carrier-iq-how-to-find-it-and-how-to-deal-with-it/

Nota: La inclusión de este *software* (API) en el ETM debe ser informada al Usuario Final, quien podría autorizar el monitoreo de su ETM y la información que podría ser enviada al Operador.

6.4.14 Sobre el Firmware y su contribución para preservar la integridad del ETM

Los fabricantes de ETM podrían implementar las siguientes recomendaciones que involucran al *Firmware*, con el propósito de coadyuvar a proporcionar evidencia sobre la seguridad del ETM.

I. **Integridad:** Un ETM puede proporcionar evidencia de que ha conservado su integridad si es capaz de demostrar que sus configuraciones de *hardware, software y Firmware* se encuentran en un estado de confianza. La integridad en el ETM es la ausencia de fallas en las configuraciones antes señaladas. Un ETM que demuestra su integridad brinda a las partes interesadas una cadena de confianza para la toma de decisiones sobre las posibles interacciones con el ETM.[75]

II. **Capacidad de aislamiento**: Implementar y preservar la capacidad de aislamiento o de separación que proporciona el *Firmware* en el ETM (en conjunto con el SO móvil) previene comportamientos maliciosos, mediante el control de las interacciones entre los Usuarios Finales y las aplicaciones móviles, y entre las aplicaciones móviles y los componentes de *hardware* del ETM.

III. **Capacidad de almacenamiento protegido**: Implementar y preservar, el almacenamiento protegido coadyuvará a preservar la confidencialidad, integridad y disponibilidad de la información almacenada en éste o que se encuentran en uso; lo anterior, en caso de que una aplicación móvil no cuente con la autorización de acceso a cierta información almacenada de forma protegida, esta capacidad podrá negar el acceso a la referida aplicación.

Ahora bien, para coadyuvar a la resiliencia del *Firmware,* se podrán emplear Módulos de seguridad de:

a. Actualización, el cual es responsable de autenticar las actualizaciones del *Firmware* y los cambios de datos críticos para respaldar las capacidades de protección del ETM;
b. Detección, el cual se responsable de las capacidades de detección de corrupción de datos críticos y del *Firmware;*
c. Recuperación, que se encarga en caso de detectar corrupción en los datos críticos y en el *Firmware* de recuperarse.

[75] https://csrc.nist.gov/CSRC/media/Publications/sp/800-164/draft/documents/sp800_164_draft.pdf

6.5 Sobre las Redes de Telecomunicaciones

6.5.1 Cifrado de las comunicaciones

Los Operadores buscarán habilitar en todo momento el cifrado de la información extremo a extremo en los ETM; lo anterior mediante los equipos de protección de seguridad de la red a efecto de coadyuvar con la confidencialidad, integridad y disponibilidad de la información.[76]

6.5.2 Gestionar un intercambio y reciclaje de la Tarjeta SIM/UICC seguro

Los Operadores, buscarán implementar un proceso de verificación de la identidad del Usuario Final antes de realizar cualquier intercambio, desbloqueo o reemplazo de la Tarjeta SIM/UICC.[77] El proceso anterior, podrá verificarse mediante autenticación de 3 pasos que consiste en algo que es, algo que tiene y algo que conoce el Usuario Final. Por ejemplo, con la verificación biométrica, la presentación de una identificación válida y el conocimiento sobre los detalles de la cuenta respectivamente.

6.5.3 Mecanismos de Almacenamiento de Tarjeta SIM/UICC

Los Operadores buscarán emplear mecanismos para proteger y almacenar de forma segura la información almacenada en la Tarjeta SIM/UICC, como son el IMSI y las claves secretas, así como contar con políticas de protección de la información para la autenticación en el HSS.[78]

6.5.4 Detectar Malware en el ETM

Los Operadores podrán poner a disposición de los Usuarios Finales un servicio de notificaciones en caso de detección de *Malware* en aplicaciones móviles descubiertas con ayuda de los equipos de protección de seguridad de la red del Operador.[79]

6.5.5 Usar red de atracción

[76] https://www.itu.int/rec/T-REC-X.1213/recommendation.asp?lang=es&parent=T-REC-X.1213-201709-I
[77] https://www.itu.int/en/publications/Documents/tsb/2019-Technical-report-on-SS7-vulnerabilities/index.html
[78] https://www.dhs.gov/publication/st-mobile-device-security-study
[79] https://www.itu.int/rec/T-REC-X.1213/recommendation.asp?lang=es&parent=T-REC-X.1213-201709-I

Los Operadores procurarán emplear redes de atracción (señuelo)[80] a efecto de propiciar el acceso de Botnets y Malware al ETM; lo anterior, a efecto de conocer el modo de operación de estos y así prevenir futuros ataques.[81]

6.5.6 Protegerse contra ataques DDoS

Los Operadores podrán contar con una política de Seguridad de la Información a efecto de que los dispositivos de protección de seguridad de la red impidan que los ETM con *Malware* de *Botnet* se conecten y se coordinen entre sí para lanzar ataques de tipo DDoS. Lo anterior, previa notificación al Usuario Final.[82]

6.5.7 Detectar y eliminar SMS no deseados

Los Operadores procurarán disponer de mecanismos para detectar y eliminar SMS no deseados enviados de forma masiva (bloqueo del spam); lo anterior, a efecto de evitar el colapso del ETM y de la red causado por la recepción masiva de dichos mensajes; asimismo los Operadores podrán enviar un mensaje de alerta informando al Usuario Final de esta situación.[83]

6.5.8 Implementar listas negras

Los Operadores buscarán emplear dispositivos de protección de seguridad de la red con la capacidad de identificar e incorporar sitios de Internet con *Malware* en sus listas negras. Lo anterior, coadyuvará a mitigar la creación *Botnets*.[84]

6.5.9 Cadena de distribución de la Tarjeta SIM/UICC

I. Los Operadores podrán solicitar a las partes interesadas la aplicación de mecanismos seguros para la fabricación, transportación, distribución e instalación de tarjetas SIM/UICC en entornos seguro.

II. Los Operadores podrán solicitar a las partes interesadas la fabricación de Tarjetas SIM/USIM empleando las especificaciones establecidas por la 3GPP.[85]

---

[80] https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot
[81] https://www.itu.int/rec/T-REC-X.1213/recommendation.asp?lang=es&parent=T-REC-X.1213-201709-I
[82] https://www.itu.int/rec/T-REC-X.1213/recommendation.asp?lang=es&parent=T-REC-X.1213-201709-I
[83] Ídem
[84] Ídem
[85] https://www.etsi.org/deliver/etsi_ts/121100_121199/121111/16.01.00_60/ts_121111v160100p.pdf

6.5.10 Implementación del uso de eSIM

Los Operadores buscarán robustecer la seguridad en los ETM mediante el uso de eSIM. La cual podrá ser descargada de forma remota en un Módulo de seguridad.

6.5.11 Confidencialidad de los datos personales

La confidencialidad de los datos personales transmitidos entre los ETM y los proveedores de Servicios de valor agregado buscarán protegerse mediante las mejores prácticas de criptografía, conforme a las propiedades de la tecnología, el riesgo y uso del ETM y de conformidad con la legislación que en materia de datos personales resulte aplicable.[86]

6.5.12 Información clara y transparente

Los fabricantes de ETM, las personas físicas o morales que desarrollen y proporcionen servicios y aplicaciones para los ETM, (proveedores de servicios de valor agregado) así como a los Operadores procurarán proporcionar a los Usuarios Finales información clara y transparente sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines, por ETM y en cada servicio, sin perjuicio de la observancia de otros o de los demás principios aplicables al tratamiento de datos personales y 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.

6.5.13 Consentimiento de los Usuarios Finales

I. Para el tratamiento de los datos personales se requiere el consentimiento de los Usuarios Finales, de conformidad con las formalidades previstas en la legislación que en materia de datos personales resulte aplicable.

II. Los Usuarios Finales que hayan otorgado su consentimiento a los Fabricantes de ETM y a los proveedores de servicios de valor agregado 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 ETM y los proveedores de servicios de valor agregado, garantizarán que los datos personales sean tratados de conformidad con la legislación que en materia de datos personales resulte aplicable.
NOTA: Es necesario señalar que una vez revocado el consentimiento los Usuarios Finales no podrán seguir empleando ciertas aplicaciones y/o funcionalidades del ETM.

[86] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

III. La obtención del consentimiento del Usuario Final 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, éste debe de ser recabado nuevamente; se deberán proporcionar a los Usuarios Finales los medios para preservar la privacidad de éstos mediante la configuración del ETM y la adecuada funcionalidad de los servicios de valor agregado y de conformidad con la legislación que en materia de datos personales resulte aplicable.

6.6 Sobre la configuración para eliminar Información Personal

En caso de robo o extravío y que el ETM cuente con todos los elementos necesarios, los Usuarios Finales buscarán realizar la eliminación automática y remota de su Información Personal almacenada en el ETM; una vez activa dicha funcionalidad, toda la información relacionada con las aplicaciones móviles, registros de llamadas de voz y datos, mensajes de texto, claves, credenciales, etc., serán eliminadas por completo del ETM cuando se conecte a Internet[87].

La Información Personal almacenada en los ETM y en los servicios de valor agregado procurarán configurarse de manera que puedan ser eliminados:

I. Fácilmente por los Usuarios Finales.
II. En el caso de una transferencia de la propiedad a otro Usuario Final del ETM o de los servicios de valor agregado.
III. Cuando el Usuario Final elimine un Servicio de valor agregado del ETM, y
IV. Cuando el ETM llegue al fin de su vida útil.

6.7 Sobre la información disponible en el portal de Internet del Instituto que coadyuva al desarrollo de una cultura de ciberseguridad.

El Usuario Final podrá consultar en el portal de Internet del Instituto, el micrositio disponible en https://ciberseguridad.ift.org.mx/ en el cual se establece información útil y practica sobre la protección de sus dispositivos, la información transmitida y/o almacenada; así como alertar sobre los riesgos de seguridad que hay en el Internet mediante el uso de sus ETM; dicha información se encuentra clasificada por temas: riesgos, consejos o recomendaciones, sitios de interés, guías y estudios y, recomendaciones del uso seguro de los ETM, aplicaciones, y software de ciberseguridad.

[87] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

7. Bibliografía

Bluetooth. (s.f.). *Origin of the Bluetooth Name.* Obtenido de https://www.bluetooth.com/about-us/bluetooth-origin/

Bluetooth. (s.f.). *Reporting Security Vulnerabilities.* Obtenido de https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/reporting-security/

Check Point. (s.f.). *Man-in-the-Disk: A New Attack Surface for Android Apps.* Obtenido de https://blog.checkpoint.com/2018/08/12/man-in-the-disk-a-new-attack-surface-for-android-apps/

CTIA. (s.f.). *Today's Mobile Cybersecurity.* Obtenido de http://files.ctia.org/pdf/CTIA_TodaysMobileCybersecurity.pdf

DHS. (Abril de 2017). *Study on Mobile Device Security. Department of Homeland Security, Science and Technology Directorate.* Obtenido de https://www.dhs.gov/publication/st-mobile-device-security-study

ENISA. (19 de Diciembre de 2012). *Consumerization of IT: Risk Mitigation Strategies*. Obtenido de https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-thematic-landscapes/COITMitigationStategiesPublishedVersion.pdf

ENISA. (19 de Diciembre de 2012). *Consumerization of IT: Risk Mitigation Strategies*. Obtenido de https://www.enisa.europa.eu/publications/COIT_Mitigation_Strategies_Final_Report/at_download/fullReport

ETSI. (2008). *Universal Mobile Telecommunications System (UMTS);USIM and IC card requirements.* Obtenido de https://www.etsi.org/deliver/etsi_ts/121100_121199/121111/08.00.01_60/ts_121111v080001p.pdf

ETSI. (02 de 2019). *ETSI TS 103 645 V1.1.1. "CYBER; Cyber Security for Consumer Internet of Things." Feb 2019.* Obtenido de https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

ETSI. (06 de 2020). *ETSI TS 103 645 V2.1.2 Cyber Security for Consumer Internet of Things: Baseline Requirements* . Obtenido de https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf

GSMA. (2016). *La Economía Móvil.* Obtenido de https://www.gsma.com/latinamerica/wp-content/uploads/2016/09/ME_LATAM_2016-Spanish-Report-FINAL-Web-Singles-1.pdf

GSMA. (03 de 2018). *eSIM Whitepaper The what and how of Remote SIM Provisioning.* Obtenido de https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf

IFT. (01 de 08 de 2016). *Disposición Técnica IFT-010-2016.* Obtenido de http://www.ift.org.mx/sites/default/files/dt-010-2016.pdf

IFT. (s.f.). *IMEI.* Obtenido de http://www.ift.org.mx/usuarios-y-audiencias/imei

ISO/IEC. (Julio de 2012)). *ISO/IEC 27032, Information technology — Security techniques — Guidelines for cybersecurity*.

ITU. (2007). *Guía de ciberseguridad para los países en desarrollo*. Obtenido de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2007-PDF-S.pdf

ITU. (04 de 2008). *Recomendación UIT-T X.1205 Aspectos generales de la ciberseguridad*. Obtenido de https://www.itu.int/rec/T-REC-X.1205-200804-I/es

ITU. (04 de 2009). *EL CIBERDELITO: GUÍA PARA LOS PAÍSES EN DESARROLLO.* Obtenido de https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

ITU. (septiembre de 2014). *X.1211 SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD Técnicas para prevenir ataques en la web*. Obtenido de https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1211-201409-I!!PDF-S&type=items

ITU. (marzo de 2016). *X.1521 SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD Sistema común de puntuación de vulnerabilidades 3.0*. Obtenido de https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1521-201603-I!!PDF-S&type=items

ITU. (septiembre de 2017). *X.1127 Requisitos de seguridad y arquitecturas funcionales para las medidas de lucha contra el robo de teléfonos móviles*. Obtenido de https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1127-201709-I!!PDF-S&type=items

ITU. (septiembre de 2017). *X.1213, SERIE X: Redes de Datos, Comunicaciones de Sistema Abiertos y Seguridad. Capacidades de seguridad necesarias para luchar contra las redes robot en teléfonos inteligentes* . Obtenido de https://www.itu.int/rec/T-REC-X.1213/recommendation.asp?lang=es&parent=T-REC-X.1213-201709-I

ITU. (2020). *Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions de la iniciativa "Financial Inclusion Global Initiative" del año 2020*. Obtenido de https://figi.itu.int/wp-content/uploads/2021/04/Technical-report-on-the-SS7-vulnerabilities-and-their-impact-on-DFS-transactions_f-1-1.pdf

ITU. (03 de noviembre de 2020). *TR-USM Unified security model (USM) – A neutral integrated system approach to cybersecurity*. Obtenido de https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-SEC.USM-2020-PDF-E.pdf

kaspersky. (2020). *Top 7 Mobile Security Threats in 2020.* Obtenido de https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store

kaspersky. (s.f.). *How to Avoid Public WiFi Security Risks.* Obtenido de https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

Komarov, A. (26 de Mayo de 2016). *Charging your smartphone's battery over USB can be dangerous.* Obtenido de https://usa.kaspersky.com/blog/usb-battery-charging-unsecurity/7195/

Luke Bencie, C. M. (30 de 11 de 2017). *Hackers Are Targeting Your Mobile Phone. Here Are 15 Ways to Slow Them Down.* Obtenido de https://hbr.org/2017/11/hackers-are-targeting-your-mobile-phone-here-are-15-ways-to-slow-them-down

McAfee Labs. (s.f.). *McAfee Labs Threats Report.* Obtenido de https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2017.pdf

MinisterioDefensa, E. (12 de 2010). *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*. Obtenido de https://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

NFC Forum. (s.f.). *What is NFC?* Obtenido de Bluetooth. (s.f.). Reporting Security Vulnerabilities. Obtenido de https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/reporting-security/

NIAP. (s.f.). *Lista de productos compatibles*. Obtenido de https://www.niap-ccevs.org/Product/

NIST. (s.f.). *Guide to Bluetooth Security National Institute of Standards and Technology.* Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

NIST. (Octubre de 2012). *Special Publication 800-164, Guidelines on Hardware- Rooted Security in Mobile Devices (Draft).* Obtenido de https://csrc.nist.gov/CSRC/media/Publications/sp/800-164/draft/documents/sp800_164_draft.pdf

NIST. (septiembre de 2016). *Draft NISTIR 8144 Assessing Threats to Mobile Devices & Infrastructure*. Obtenido de https://csrc.nist.gov/CSRC/media/Publications/nistir/8144/draft/documents/nistir8144_draft.pdf

NIST. (21 de Diciembre de 2017). *Guide to LTE Security, NIST Special Publication (SP) 800-187.* Obtenido de https://csrc.nist.gov/csrc/media/publications/sp/800-187/draft/documents/sp800_187_draft.pdf

NIST. (07 de 2017). *Special Publication 800-63B Digital Identity Guidelines*. Obtenido de https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf

NIST. (Mayo de 2018). *Platform Firmware Resiliency Guidelines*. Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

NIST. (s.f.). *Guidelines for Securing Radio Frequency Identification (RFID) Systems National Institute of Standards and Technology*. Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-98.pdf

SD Asociacion. (23 de septiembre de 2020). *Part1 Physical Layer Simplified Specification Ver8.00*. Obtenido de https://www.sdcard.org/downloads/pls/pdf/?p=Part1_Physical_Layer_Simplified_Specification_Ver8.00.jpg&f=Part1_Physical_Layer_Simplified_Specification_Ver8.00.pdf&e=EN_SS1_8

SD Association. (2000). *About the SD Association.* Obtenido de https://www.sdcard.org/about-sda/

Security, D. o. (abril de 2017). *Study on Mobile Device Security.* Obtenido de https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf

ift INSTITUTO FEDERAL DE TELECOMUNICACIONES

CÓDIGO DE MEJORES PRÁCTICAS **PARA LA CIBERSEGURIDAD EN** EQUIPOS TERMINALES MÓVILES

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