ift INSTITUTO FEDERAL DE TELECOMUNICACIONES

La **Ciberseguridad** en las **Redes Móviles** y la **responsabilidad compartida**

2023

Contenido

Introducción

El Instituto Federal de Telecomunicaciones y la industria, unen esfuerzos y recursos con el propósito de proporcionar elementos de información a aquellos interesados en conocer los diferentes aspectos de la ciberseguridad, en particular en su aplicación en las redes móviles de telecomunicaciones y con ello, promover que la ciberseguridad sea una práctica cotidiana en el ecosistema digital en beneficio de las personas usuarias. Con este objetivo se pone a disposición del público interesado este material informativo y de consulta profesional, en el que se podrá encontrar fuentes de información de tipo técnico que brindan una orientación a aquellas personas interesadas en profundizar en temas relacionados con la seguridad digital.

Hacia un mundo digital inteligente totalmente conectado

Los avances de la humanidad en tecnologías digitales nos van llevando a escenarios nunca antes imaginados. Hoy día tenemos aplicaciones en tiempo real en donde se reducen o eliminan los tiempos de espera, filas, papeleo, y otros inconvenientes en la provisión de servicios cuando y donde se necesiten. La conveniencia de las comunicaciones inalámbricas se expande a transferencias de datos de banda ancha, con mínimos tiempos de retardo y con capacidad de conexiones masivas de dispositivos de máquinas o cosas, estos avances se reflejan en áreas como: **los servicios de salud se van digitalizando, el sector agrícola estará automatizando y optimizando sus procesos de distribución, la evolución de los vehículos para ser auto conducidos, los servicios financieros e intercambio de valores se realizan en tiempo real y sin fronteras, las ciudades totalmente interconectadas para soportar sistemas inteligentes que proporcionan servicios más eficientes, así como el impacto de la transformación digital en las funciones de la administración pública y gobierno.** En resumen, estamos en la era de un mundo digital inteligente totalmente conectado.

Este panorama conlleva el reto de generar un entorno de confianza y seguridad en los sistemas y servicios de telecomunicaciones móviles para las personas usuarias. Para hacer una explicación de cómo se organizan los sistemas de la red móvil y como se garantiza su seguridad podemos mencionar que existen tres aspectos a considerar:

- **Seguridad de las aplicaciones,**
- **Seguridad de la Red y operadores de servicios y**
- **Seguridad de elementos de Red.**

Este estudio se centra en los dos últimos, debido a que constituyen la base para garantizar un ecosistema más confiable. En siguientes líneas se presentará de manera sencilla un panorama de cómo los fabricantes y operadores de redes móviles trabajan con base en estándares y mejores prácticas con el propósito de generar soluciones y servicios confiables y que les permita tener continuidad de servicios ante posibles amenazas o vulnerabilidades.

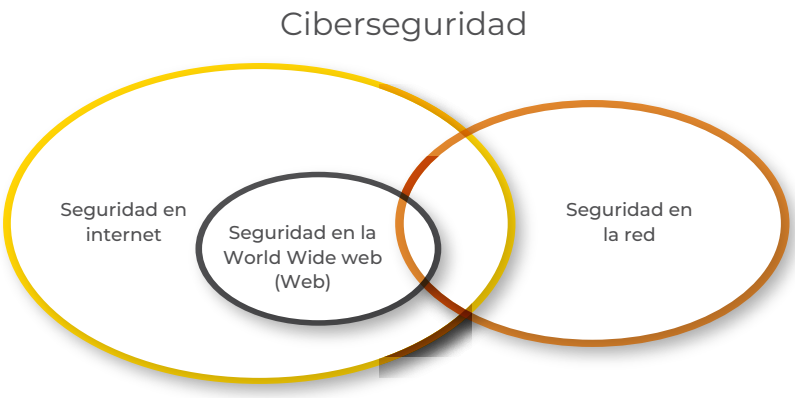
Nuevas tecnologías, nuevas aplicaciones y los retos de la ciberseguridad de las redes móviles

El uso de las nuevas tecnologías y el acceso a internet cada vez más asequible ha llevado a las personas que se conectan al internet a estar en una situación vulnerable frente a amenazas en línea: ya sea robo de identidad, engaños, fraudes, ciberbullying, extorsión, e incluso vigilancia constante de su día a día. Por ello, es importante que las personas usuarias conozcan las mejores prácticas para aprender ciberseguridad en la tecnología para su uso en forma segura.

La ciberseguridad se centra en los mecanismos y prácticas que sirven para proteger a quienes usan los dispositivos y su privacidad cuando navegamos en el internet.

A diferencia de lo que podamos pensar, la ciberseguridad no requiere de grandes conocimientos informáticos o sobre redes, ni tampoco requiere equipos muy sofisticados en tecnología, tan solo requiere los dispositivos, sentido común y formar hábitos siguiendo mejores prácticas. Con esto podemos convertirnos en personas usuarias. No importa la edad, ni los conocimientos que se tengan, ¡la ciberseguridad es para todas y todos!

La relación entre la seguridad del Internet, la seguridad en la Web, la seguridad de Redes y la Ciberseguridad



El **Internet** es un sistema global de redes digitales interconectadas en el dominio público. El intercambio de información a través del Internet también utiliza las redes públicas de telecomunicaciones móviles, por lo tanto, forma parte de Internet. El internet conecta miles de millones de servidores, computadoras y otros dispositivos con tecnología para conectarse al internet. Cada dispositivo está conectado con cualquier otro dispositivo a través de su conexión a Internet. Internet crea el entorno para el sistema de intercambio de información posible en la web. En ese sentido, la seguridad de Internet se ocupa de proteger los servicios relacionados con Internet y los sistemas y redes de tecnologías de información y comunicación conexos como una extensión de la seguridad de la red, a fin de reducir los riesgos de seguridad relacionados con Internet para los las personas usuarias.

La **Web**, como abreviatura de World Wide Web, es una de las formas en que la información se comparte en Internet (otras incluyen el correo electrónico, transferencia de archivos y servicios de mensajería instantánea). La web se compone de miles de millones de documentos digitales conectados que se pueden ver mediante un navegador web. Un sitio web es un conjunto de páginas web relacionadas que se preparan y mantienen como una colección en apoyo de un único propósito.

La **seguridad web** se ocupa de la seguridad de la información en el contexto de la World Wide Web (WWW) y de los servicios web a los que se accede a través de la red pública.

Una **Red** se compone de elementos de red, tales como: equipos de acceso Wi-Fi, radio-bases para acceso inalámbrico con tecnología celular de 3G, 4G, y 5G, microondas, equipos para iluminación de fibra óptica, enrutadores, concentradores, controladores y centrales de telecomunicaciones, centros de datos, y dispositivos de control técnico. Por lo tanto, la seguridad de la red cubre todo tipo de redes que existen dentro de una organización desde la red de área local, la red de área metropolitana, las redes privadas y las redes inalámbricas.

La **ciberseguridad** se refiere a la gestión de los riesgos de seguridad de la información cuando la información está en forma digital en computadoras, almacenamiento local o en la nube y redes. Muchos de los controles, métodos y técnicas de seguridad de la información se pueden aplicar para gestionar los riesgos cibernéticos.

La ciberseguridad también es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. La ciberseguridad se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes.

Mejores prácticas internacionales para la Ciberseguridad en las redes de telecomunicaciones e internet móvil

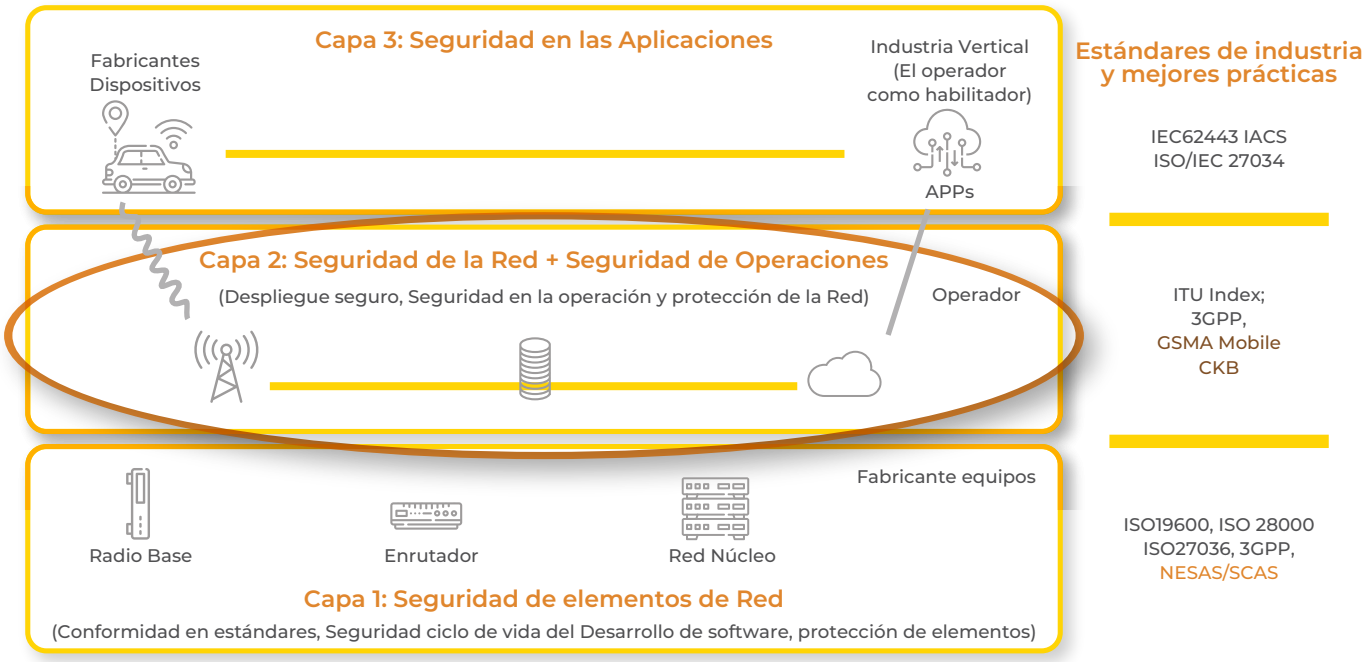
Con el despliegue y operación de redes móviles de 3G, las personas usuarias pueden acceder al internet en forma inalámbrica móvil, y con las evoluciones a 4G y 5G se potencializó una infinidad de servicios digitales: redes sociales, banca en línea, compras en línea, reuniones interactivas con video, videos de entretenimiento o aprendizaje bajo demanda, automatización de cosas a través de dispositivos, etc.

La ciberseguridad en las redes se enfrenta a múltiples amenazas y desafíos de seguridad. Para ayudar a los operadores, desarrolladores de aplicaciones y fabricantes en el ecosistema móvil, la Asociación GSMA, una organización global que asocia las empresas del ecosistema de Telecomunicaciones Móviles (GSMA) ha llevado a cabo un análisis integral de amenazas, así como la recopilación de información de fuentes públicas de organizaciones de estándares y especificaciones técnicas. Esta recopilación y análisis se constituye en un conjunto de documentos denominado Base de conocimientos sobre ciberseguridad móvil[1], el cual proporciona orientación útil sobre una serie de riesgos y medidas de mitigación. La base de conocimientos, sigue la estructura del modelo de seguridad de tres capas del ecosistema móvil, que a su vez define la distribución de responsabilidades compartidas y contribuye a que el mundo interconectado sea lo más seguro posible. Como un documento vivo, con el tiempo, la base de conocimientos se va actualizando, mejorando y ampliando para responder a la evolución del panorama de las amenazas a la ciberseguridad.

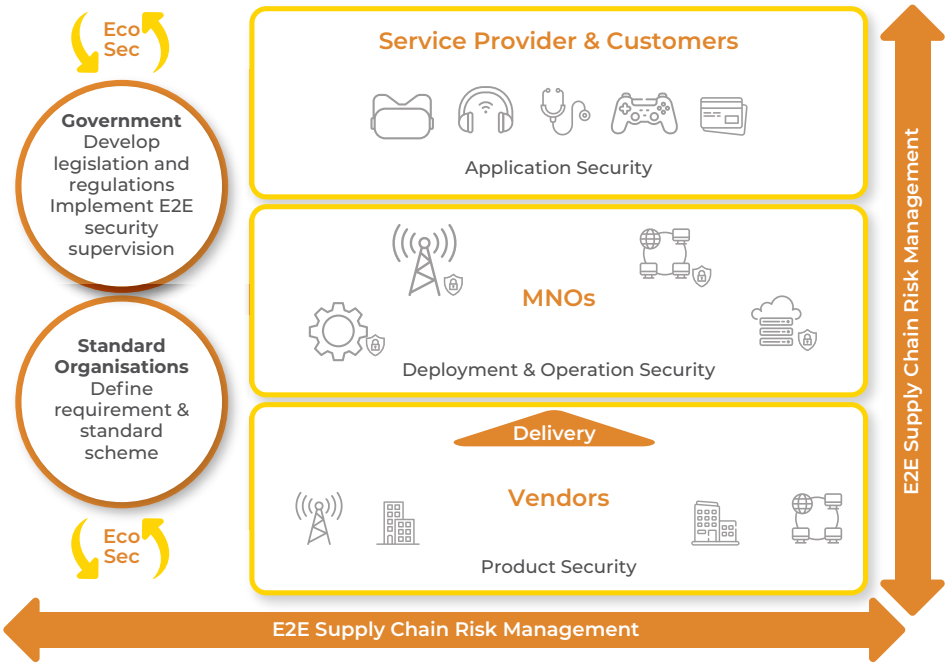
1 https://www.gsma.com/security/mobile-cybersecurity-knowledge-base/

El modelo de seguridad de 3 capas es ampliamente aceptado en la industria de las telecomunicaciones, incluyendo 3GPP, 5GPPP, etc.

La ciberseguridad móvil requiere responsabilidad compartida entre los diferentes actores.



La base de conocimientos sobre ciberseguridad móvil constituye un panorama integral de amenazas diseñado para ayudar a múltiples organizaciones (operadores, proveedores de equipos, reguladores, desarrolladores de aplicaciones y proveedores de servicios) a comprender las amenazas a la seguridad que plantean las redes móviles de manera sistemática y objetiva.



Los operadores de redes, están desarrollando competencias y capacidades de seguridad móvil que, a nivel operativo, significa contar con instrucciones claras para tomar medidas paso a paso para crear garantías de seguridad, teniendo en cuenta todo el espectro de riesgos de las redes móviles de extremo a extremo. Esto contribuirá a construir la confianza con las personas usuarias, las empresas, y aquellas organizaciones que utilizan servicios digitales.

En resumen, la seguridad debe tener un principio de transparencia en los esfuerzos de todos los jugadores. Para el caso de la capa de redes públicas, la Base de conocimientos de ciberseguridad de la GSMA contribuye en la seguridad de extremo a extremo: seguridad para la planificación, construcción, mantenimiento, optimización y operación de la red; es una guía de referencia para la industria. Esta base de conocimientos se construyó con la colaboración de la industria, reguladores, operadores, fabricantes de equipos, proveedores de servicios, y desarrolladores de aplicaciones, todos trabajando juntos para cumplir con los requisitos de seguridad establecidos por la base de conocimientos. La Base de Conocimientos fue publicada oficialmente en el mes de Mayo del 2021, y se esta actualizando como un documento vivo.

Finalmente, se puede tener una evaluación de seguridad en la que los operadores pueden implementar medidas de control de seguridad y realizar una evaluación basada en el modelo de madurez de seguridad que forma parte de la Base de Conocimientos de la GSMA. La guía para hacer la evaluación se encuentra en el documento "Linea Base de Controles de Seguridad FS31", ver aquí:

"FS.31 GSMA Baseline Security Controls"

Para más información ir a:

Base de Conocimientos de la Ciberseguridad en Red Movil de la GSMA.

English: GSMA Mobile Cybersecurity Knowledge Base