Fraude y medidas de Seguridad en transacciones a través de Servicios Digitales Financieros (DFS)

Alejandro Corletti Estrada
acorletti@darFe.es
www.darFe.es

Presentación del tema

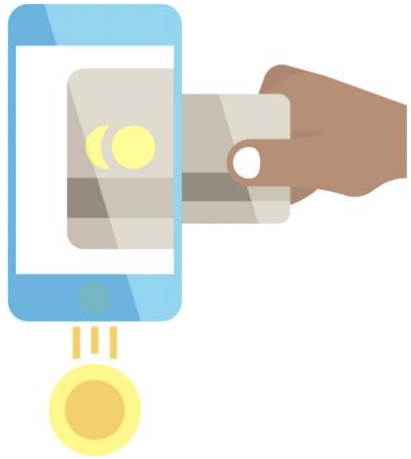
Nos encontramos ante un nuevo paradigma o nicho de mercado donde, los tradicionales servicios financieros, están migrando hacia servicios dependientes cien por ciento de las Telecomunicaciones.

Las autoridades y grandes holdings financieros están empujando fuertemente a la sociedad y empresas a hacer uso de ellos, pues les conviene en todo sentido.

El crecimiento de estos **Servicios Digitales Financieros** es vertiginoso, pero… El Usuario, la Banca y los Gobiernos necesitan y exigen **SEGURIDAD** y la masa de la responsabilidad sobre este tema la tienen las **"Telco"**.

En este texto, se trata de resumir el problema y sus potenciales soluciones a través del siguiente temario:

1. Fintech.
2. Dar forma al futuro de los servicios financieros en la economía digital.
3. ¿Qué son los Servicios Financieros Digitales? *(**DFS**: Digital Financial Services).*
4. ¿Por qué nos interesa todo lo desarrollado anteriormente?
5. El problema concreto de la seguridad y su evolución hacia entornos seguros.
6. Mejores Prácticas.
7. Conclusiones finales.



1. Fintech.

"Fintech" es un término amplio que define el uso de aplicaciones digitales, software, tecnología digital por parte de organizaciones financieras, bancos y startups. Pueden ir desde servicios de pagos, como ***Bizum*** o ***Twyp***, hasta sistemas de crédito al consumo como ***Movistar Money***.

Tendencias de Servicios Financieros.

La industria de servicios financieros, especialmente la industria bancaria, se está convirtiendo cada vez más en un negocio de tecnología. Más que nunca, la competitividad de varios productos centrados en las finanzas se diferencia por las soluciones tecnológicas que los habilitan [1].

Fintech en mercados emergentes.

Otro factor importante que dio forma al rostro de las Fintech es la penetración de los teléfonos inteligentes en el mercado masivo que ha permitido el acceso a Internet para millones de personas en todo el mundo. Los teléfonos inteligentes también se han convertido en el **medio principal** por el cual las personas acceden a Internet y utilizan diferentes servicios financieros.

La forma en que los teléfonos móviles han cambiado el comportamiento de los consumidores y en que las personas acceden a Internet es también la razón por la que en la tabla siguiente se diferencian entre los países desarrollados y en desarrollo y hablan de **Fintech 3.5** cuando se trata de estos últimos.

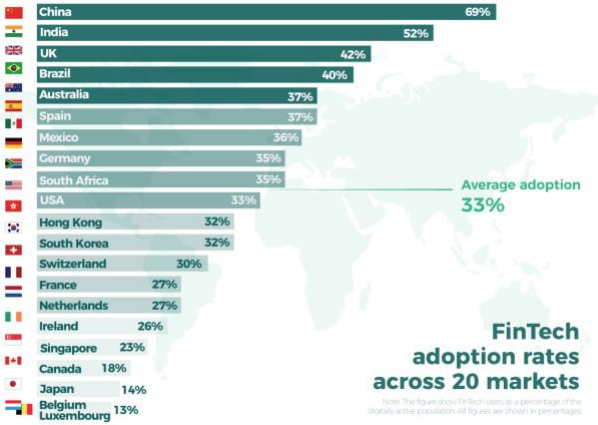


*Imagen tomada del documento "**Evolution of Fintech**" (https://www.e-zigurat.com/innovation-school/blog/evolution-of-fintech/).*

2. Dar forma al futuro de los servicios financieros en la economía digital.

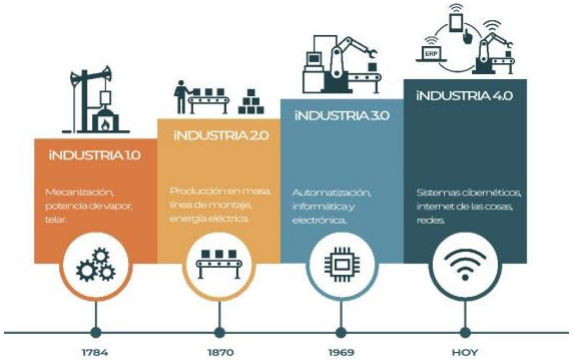
Según las actas de la Cuarta Cumbre de Políticas y Conocimiento entre América Latina y el Caribe y China [2].

[1] https://www.f5.com/c/landing/BFSI/article/banking-on-digital-transformation-the-evolution-of-US-financial-services

[2] https://publications.iadb.org/publications/english/document/Shaping_the_Future_of_Financial_Services_in_the_Digital_Economy_Proceedings_from_the_Fourth_Policy_Knowledge_Summit_between_Latin_America_and_the_Caribbean_and_China_en.pdf

RESUMEN: El crecimiento exponencial de la digitalización y la conectividad a Internet es la columna vertebral de la **Cuarta Revolución Industrial**, que ha afectado a todos los sectores, incluidos los servicios financieros. La economía digital ha impactado profundamente el sector de servicios financieros en China al permitir nuevos modelos de negocios de banca e inversión basados en Internet con un menor costo de operación que han ampliado significativamente el alcance entre los consumidores.

"China ve la **economía digital** como un nuevo paradigma económico que diversifica aún más las actividades económicas, protege el mercado nacional de posibles choques externos y permite la mejora de las condiciones de vida de las personas y las empresas por igual".



De estas actas se desea remarcar especialmente el **Panel 4** (Página 43): "**ADAPTATION OF TELECOMMUNICATIONS OPERATORS TO THE INTERNET FINANCE ECOSYSTEM**" (*por Mr. Zhang Xiaorong, Research Institute, Telecom Beijing*)

El resumen de conceptos es el siguiente:

Para analizar el papel de los operadores de telecomunicaciones en el ecosistema Fintech, es necesario tener en cuenta que las empresas que quieren realizar pagos digitales tienen estrategias de negocio específicas, que deben alinearse con los objetivos del operador (**Telco**).

Un factor clave es que la **tarjeta SIM** se puede utilizar para registrar cuentas y así realizar diferentes tipos de pagos.

Orange en Francia ha sido uno de los pocos proyectos exitosos en el desarrollo de una billetera móvil: creció un 60 por ciento anual. **Aumenta la seguridad del cliente, lo que se ha traducido en retención**.

3. ¿Qué son los Servicios Financieros Digitales? (**DFS**: Digital Financial Services).

Los servicios financieros digitales (**DFS**) incluyen una amplia gama de servicios a los que se accede y se prestan a través de canales digitales, incluidos pagos, crédito, ahorros, remesas y seguros. El concepto DFS incluye servicios financieros móviles (**MFS**).

MFS es el uso de un teléfono móvil para acceder a servicios financieros y ejecutar transacciones. MFS incluye: M-Banking, M-payments, M-money.

- **M-Money** es un servicio móvil que facilita las transferencias electrónicas y otros servicios que utilizan redes móviles.
- **M-payments** es el servicio concreto de pagos por móvil (ejemplo: Mobile Pay).
- **M-Banking** es el uso de un teléfono móvil para acceder a servicios bancarios y ejecutar transacciones financieras. - A menudo se utiliza para referirse solo a clientes con cuentas bancarias.

Tres modelos de negocio:

- **Modelo dirigido por el banco** (generalmente: Mobile Virtual Network Operator: **MVNO**)
- **Modelo liderado por MNO** (Mobile Network Operator) (por ejemplo, Airtel Money, MPESA)
- **Modelo independiente** (por ejemplo, bKash) no son bancos, ni MNO.

Este modelo de negocio, presenta situaciones "mix" pues hay bancos que ya son **MVNO**, como es el caso de **SberBank,** (Rusia) y hay **MNO** que buscan nichos de mercado financieros, como es el caso de **Movistar Money** (España) que ofrece financiamiento a sus subscriptores a través de "Telefónica Consumer Finance" (*Entidad financiera constituida "a pachas" entre **Telefónica** y **CaixaBank***).

Existen también importantes alianzas como es el caso de **Bizum**, conformada por la unión de 27 bancos Españoles.

Lo que se desea destacar en todos estos casos es el **doble factor de autenticación** que emplean casi todos ellos, y es el tema central que sigue en este artículo.

4. ¿Por qué nos interesa todo lo desarrollado anteriormente?

Porque en un informe reciente de **ITU**, **ENISA** y todos los organismos financieros relevantes, donde se presenta el tema del Fraude en DFS es través de dos vías (ATTACK SURFACES) [3]:

- **SS7** (*principalmente por medio de: **SMS** y **USSD** – ambos son mensajes SS7*).
- **cellular air interface**

NOTA: Estas vías incluyen también la **SIM card**.

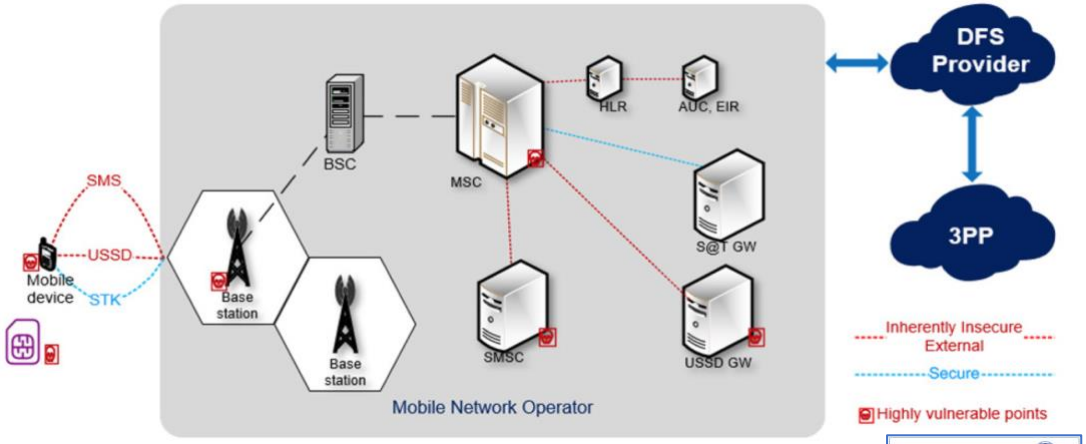


Imagen tomada del documento: 20-00383 Security testing for USSD and STK.pdf

Ver detalle en libro "**Seguridad en Redes**"

www.darFe.es

[3] https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/ITU_SIT_WG_Technical-report-on-the-0SS7-vulnerabilities-and-their-impact-on-DFS-transactions_f.pdf

*Según encuestas realizadas por este grupo de trabajo y la Agencia de la Unión Europea para la Seguridad de las Redes y la Información (**ENISA**), **menos del 30%** de las empresas de telecomunicaciones de la Unión Europea (**UE**) y menos del 0,5% de las empresas de telecomunicaciones de los países en desarrollo han implementado estas medidas de mitigación.*

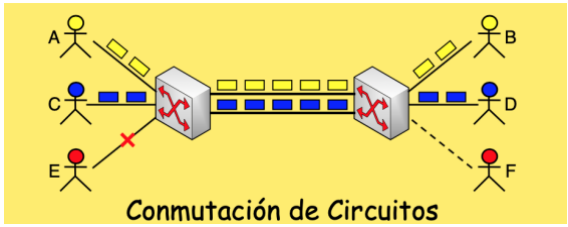
En virtud de que las **DFS** (digital financial services), **ITU** (International Telecommunication Union) y **ENISA** (European Union Agency for Network and Information Security), estén tomando participación en este fraude de SS7 y que nos indiquen que es real, de impacto y que sólo un 30 % de las medidas han sido implantadas, es más que suficiente para alertarnos que debemos incrementar (urgentemente) la seguridad de esta infraestructura de señalización.

5. El problema concreto de seguridad y su evolución hacia entornos seguros.

En estos momentos, la red mundial de Telecomunicaciones podríamos plantearla como **dos redes**, no es una sola. Ambas, si bien casi, casi, casi, casi, se trata de una única infraestructura montada sobre el protocolo **IP** (*Internet Protocol*), aún, en enero de 2021, siguen operando como dos redes diferentes (*y reitero, es así a nivel mundial, desde los países más avanzados, hasta los menos*).

Estas dos redes son:

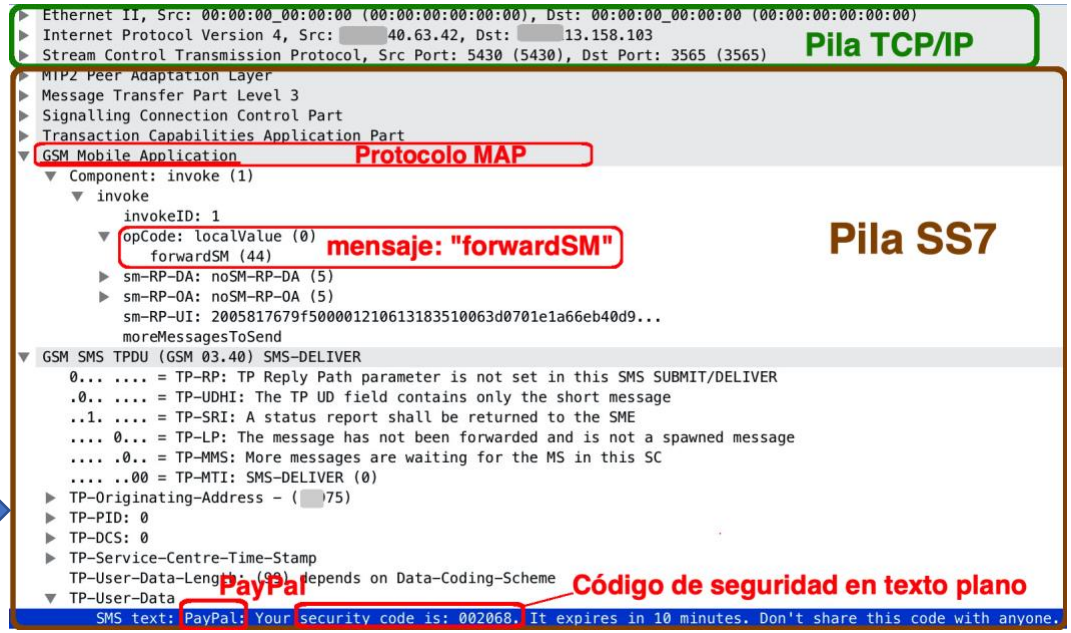
- **Red de Voz** (Técnicamente llamada de conmutación de circuitos)



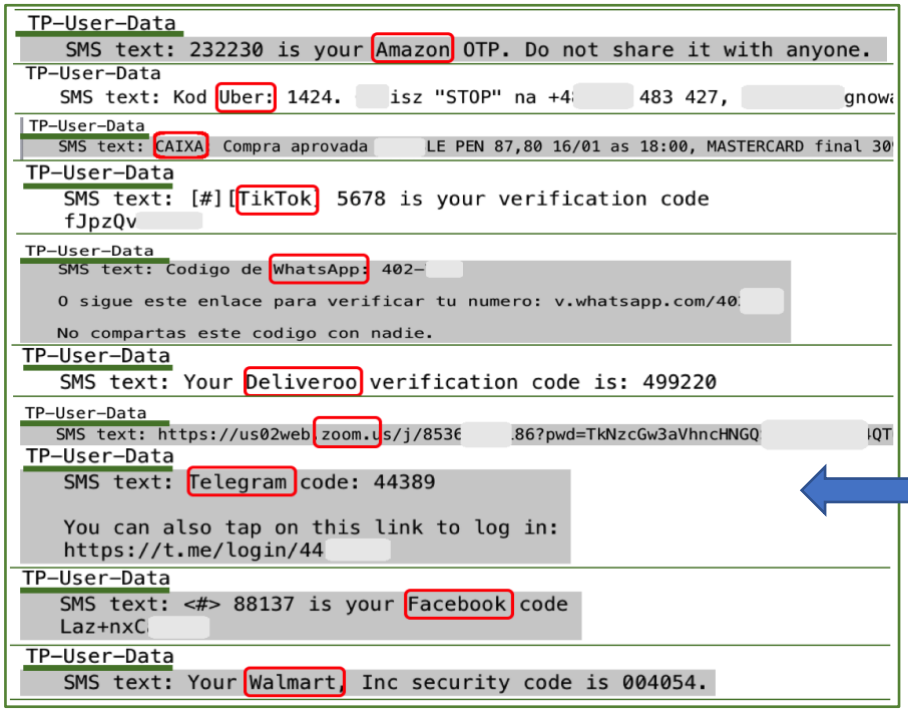
- **Red de datos** (Técnicamente llamada de conmutación de paquetes)

Ambas se unificarán a nivel mundial, únicamente cuando TODAS las operadoras del mundo tengan VoLTE (no solo 4G sin Voz sobre 4P o VoLTE) y en la red fija el 100% de fibra óptica... estamos hablando con mucha suerte de 5 años vista o más aún. Cuando así sea, toda la red será única y absolutamente de "paquetes", desechado la conmutación de circuitos. Me encantaría dedicar más tiempo a esta idea pues sería importantísimo poder bajarla al terreno humanamente entendible, pero en estas líneas, no nos dará el tiempo, podéis buscar en Internet algunos artículos que he escrito sobre el tema.

Como hemos dicho, los problemas de estos servicios financieros, van relacionados con mensajes SS7 de esta "red de voz", analicemos uno de ellos:

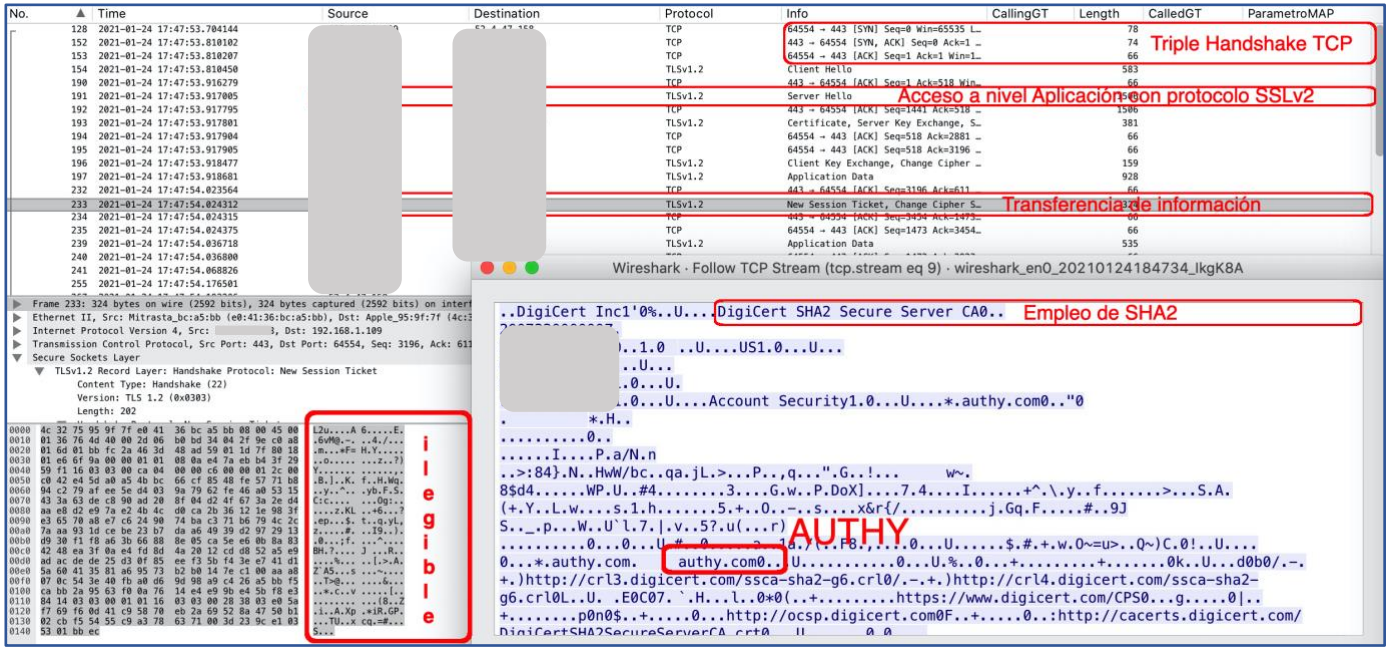


En la imagen vemos: la parte correspondiente a la pila **TCP/IP**, debajo de ella la parte de **SS7** y en este caso concreto, un mensaje SS7 cuyo "Operation Code" es: "**forwardSM**" y se corresponde con un factor de doble autenticación enviado por **PayPal**. El detalle que deseo que observéis (independientemente de las debilidades y ataques de la red SS7), es que estáis observando todo el contenido en **texto plano**.



Si analizamos únicamente el campo "**TP-User-Data**" en otras capturas de tráfico, vemos que estos mensajes SS7 en texto plano, son empleados por un sinnúmero de aplicaciones y empresas.

Comparemos un código enviado por **SS7** a través de un mensaje **SMS** contra un código generado por la red IP, a través de un **TOTP**, en este caso por medio de la aplicación "***Authy***".



En eta imagen podemos ver el triple handshake TCP, una vez finalizado ya pasa al nivel aplicación con el protocolo **SSLv2** empleando el algoritmo **SHA2**, en la ventana inferior de Wireshark, se ve perfectamente que el contenido es "**ilegible**".

En resumen, lo que se intenta presentar en los dos casos, es la gran diferencia entre continuar empleando la **red de voz** (con mensajes SS7) o ir migrando estos DFS hacia la **red de paquetes**, empleando todas las fortalezas que en la actualidad ofrece la pila **TCP/IP** (como en este caso por medio de SSL_v2).

6. Mejores Prácticas.

Como guía de mejores prácticas, se presenta a continuación exactamente lo que recomienda realizar DFS/ITU-T en su documento:

"Security Aspects of Digital Financial Services (DFS)" [4]

Los servicios financieros digitales (**DFS**) prometen permitir la inclusión financiera y pueden mejorar la seguridad física de sus usuarios. Sin embargo, las amenazas emergentes a la seguridad de DFS pueden comprometer a las partes interesadas en todos los niveles del ecosistema.

A continuación, se presenta un resumen de las recomendaciones de este documento:

[4] https://www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS_SecurityReport.pdf

R1: Considere el uso de fuertes mecanismos de autenticación para demostrar la propiedad del dispositivo.

R2: Hacer uso de mecanismos de hardware y software dentro de los dispositivos móviles, como elementos seguros y TEE (Trusted Execution Environments), que pueden garantizar la integridad del dispositivo y promover el uso de dispositivos equipados con funciones de seguridad para su uso en DFS.

R3: Ya sea que una aplicación esté diseñada para su implementación en el teléfono o en un elemento seguro, debe diseñarse e implementarse de acuerdo con las mejores prácticas, incluida la comunicación encriptada y autenticada y las prácticas de codificación segura para fortalecer la aplicación.

R4: Las aplicaciones deben someterse a una revisión de seguridad externa y pruebas de penetración, y se debe actuar sobre cualquier recomendación.

R5: Las aplicaciones deben administrar de forma segura la información de nombre de usuario y contraseña para que los adversarios no puedan falsificar las credenciales con facilidad, y deben usar mecanismos de autenticación sólidos para protegerse contra el acceso no autorizado.

R6: Las actualizaciones de seguridad periódicas son fundamentales para garantizar que los sistemas operativos móviles que se ejecutan en los dispositivos de los usuarios funcionen con los últimos parches de seguridad.

R7: Asegúrese de que las bibliotecas de seguridad que ofrece el sistema operativo estén diseñadas e implementadas correctamente y que los conjuntos de cifrado que admiten sean lo suficientemente sólidos.

R8: El sistema operativo del teléfono debe configurarse de manera que contenga el mínimo de archivos y todos confiables (es decir desinstalar cualquier programa, aplicación o script innecesario).

R9: Refuerce la seguridad de las tarjetas SIM mediante el uso de cifrados criptográficos sólidos y proteja las actualizaciones mediante técnicas de listas blancas como el filtrado en la propia red.

R10: Suspenda el uso de cifrados de cifrado GSM A5 / 0, A5 / 1 y A5 / 2.

R11: Considere la posibilidad de abandonar las aplicaciones móviles que aprovechan SMS y USSD en favor de soluciones que utilicen criptografía de clave pública sólida y seguridad de extremo a extremo.

R12: Los MNO deben implementar políticas de seguridad que mantengan la integridad de sus redes y eviten el acceso no autorizado a las cuentas de los clientes.

R13: La integridad de los sistemas DFS de back-end también debe mantenerse mediante pruebas continuas, filtrado de intrusiones y monitoreo de redes e infraestructura.

R14: Los MNO y los reguladores deben emprender campañas activas de concienciación del cliente para educar a los consumidores sobre los mensajes maliciosos, el phishing y los ataques de suplantación.

R15: Los MNO deben monitorizar las llamadas entrantes de los operadores de interconexión y realizar un análisis CLI (Caller Line ID) falso e implementar una lista blanca o negra de CLI, así como otros mecanismos de seguridad, asociados con los intentos de robar las credenciales de los clientes.

R16: El desarrollo de evaluaciones comparativas de seguridad y las pruebas periódicas de las defensas para protegerse contra nuevos ataques es vital para garantizar la confidencialidad e integridad continuas de los datos almacenados en estos entornos.

R17: Los MNO deben asegurarse de que cuando los agentes de DFS estén involucrados en operaciones de intercambio de SIM, existan mecanismos para garantizar que el propietario legal verificado reciba una nueva SIM de cliente.

R18: Los PSP deben asegurarse de que las tarjetas recargables de uso general asociadas vinculadas a las cuentas DFS requieran el uso de chips EMV (Europay MasterCard VISA) con métodos de verificación del titular de la tarjeta, como PIN o datos biométricos (cuando sea posible), y que todas las transacciones con tarjeta generen una alerta para los clientes.

R19: Emplear sólidas prácticas de criptografía para garantizar la confidencialidad e integridad de los datos cuando ingresan a la red del proveedor y cuando se procesan y almacenan en este entorno.

R20: Mantener los sistemas actualizados y monitoreados contra amenazas maliciosas de código externo y emplee rutinas de validación de entrada sólidas en servicios externos.

R21: Mantener una cadena de suministro confiable para asegurar la integridad de los sistemas que soportan DFS dentro de estas redes.

En el documento ofrece mucha más información de detalle. Además, también se proporciona un conjunto más amplio de recomendaciones basadas en la protección de los sistemas de tecnología de la información utilizados dentro y entre las partes interesadas, como los proveedores de DFS y las entidades externas. Las conclusiones resumen y encapsulan los más importantes de nuestros hallazgos, en particular la necesidad de la transmisión segura de datos entre usuarios y proveedores de datos, el uso de seguridad habilitada por hardware en dispositivos móviles para garantizar la seguridad de la información en esas plataformas, y mejores prácticas para el manejo de datos dentro de los sistemas y redes de proveedores de DFS, así como el desarrollo de evaluaciones comparativas de seguridad y pruebas regulares de defensas.

7. Conclusiones finales.

1) Es evidente que los **DFS** son uno de los mejores nichos de mercado para una MNO.
2) Existe un peligro real de perder gran parte de este nicho de negocio que lo pueden ganar otros actores (*como los citados: bancos, MNVO, Airtel Money, bKash, MPESA, Google authenticator, Criptocalculadoras Santander, etc.*).
3) La clave está, tal cual se ha mencionado en **Aumentar la seguridad del cliente, lo que se ha traducido en retención**.
4) Hay una serie de recomendaciones que son totalmente claras sobre cómo una Telco debe afrontar el problema.
5) Sobre la experiencia que se tiene en la seguridad real e implantada al día de hoy en las Teleoperadoras, se desprende tienen aún bastante camino por recorrer para cumplir el punto 3).
6) Este camino se traduce en tres líneas de acción:
   - Cumplir con máximo detalle las **21 recomendaciones** expuestas en el punto anterior.
   - **Supervisar**, **controlar** y **auditar** su cumplimiento.
   - Y lo más IMPORTANTE: Lanzar una metodología de **migración de los servicios** que actualmente se ofrecen por medio de la **red SS7 hacia la red IP**, por ejemplo, fomentando el empleo del producto ***LATCH Cloud TOTP*** de "**eleven Path**" o el mencionado ***Authy***.

Madrid, febrero de 2021.

www.darFE.es **Muchas gracias**

REFERENCIAS sobre publicaciones de DFS/ITU-T: *https://www.itu.int/pub/T-TUT-DFS/es*

Digital Financial Services (DFS)

- 2017 Digital Financial Services (DFS) - Ecosystem
- 2017 Digital Financial Services (DFS) - Consumer Experience and Protection
- 2017 Digital Financial Services (DFS) - Interoperability
- 2017 Digital Financial Services (DFS) - Technology, Innovation and Competition
- 2017 Digital Financial Services (DFS) - Recommendations
- 2017 Digital Financial Services (DFS) - Executive Summary
- 2019 DSTR-DFSECO - The digital financial services ecosystem
- 2019 DSTR-DFSREG - Regulation in the digital financial services ecosystem
- 2019 DSTR-DFSSNDL - Impact of social networks on digital liquidity
- 2019 DSTR-DFSCA - Competition aspects of digital financial services
- 2019 DSTR-DFSRP - The regulator's perspective on the right timing for inducing interoperability
- 2019 DSTR-DFSPI - Access to payment infrastructures
- 2019 DSTR-DFSUAAFR - Review of DFS user agreements in Africa: A consumer protection perspective
- 2019 DSTR-DFSCP-Commonly identified consumer protection themes for digital financial services
- 2019 DSTR-DFSMR-Main recommendations
- 2020 DFS - Digital Financial Services Consumer Competency Framework
- 2020 DFS - Security testing for USSD and STK based Digital Financial Services applications
- 2020 Technical Report on Methodology for inter-operator and cross-border P2P money transfers
- 2020 Security analysis of the KaiOS feature phone platform for DFS applications