

Clínica de Seguridad y QoS de la Iniciativa Global de Inclusión Financiera Taller para México

24 al 26 de noviembre de 2020

24 de noviembre de 2020 – Taller de QoS

<p>09:00 – 09:10</p>	<p>Inauguración</p> <ul style="list-style-type: none"> ● Javier Juárez Mojica Comisionado, Instituto Federal de Telecomunicaciones ● Bilel Jamoussi Chief of the Study Groups Department, TSB ● Sofie Maddens Head of the Regulatory and Market Environment Division, BDT
<p>09:10 – 10:30</p>	<p>Metodología para evaluar los KPI de QoS/QoE (calidad de experiencia) para los servicios financieros digitales (Parte 1)</p> <p>Los problemas de calidad de servicio (QoS, por sus siglas en inglés) pueden afectar la disponibilidad de la red móvil, lo que provoca que el consumidor no pueda completar una transacción de servicios financieros digitales (DFS, por sus siglas en inglés). El objetivo principal de de Seguridad, Infraestructura y Confianza para medir los indicadores clave de rendimiento (KPI) para la calidad del servicio de la red móvil en los servicios financieros digitales y una metodología que los reguladores de telecomunicaciones pueden utilizar para evaluar los KPI para QoS. La metodología se ha estandarizado por la Comisión de Estudio 12 del UIT-T en la esta sesión será compartir las conclusiones del estudio realizado por el Grupo de Trabajo Recomendación UIT-T P.1502.</p> <p>Panelistas</p> <ul style="list-style-type: none"> ● Kwame Baah-Acheamfour Autoridad Nacional de Comunicación, Ghana ● Dr Wolfgang Balzer Director General, Focus Infocom, Alemania

10:40 – 12:00

Metodología para evaluar los KPI de QoS/QoE para los servicios financieros digitales (Parte 2)

En la segunda parte del taller, la sesión se centrará en ampliar la metodología explicada en la parte 1 para incluir los casos de interoperabilidad y el uso transfronterizo.

Panelistas

- **Kwame Baah-Acheamfour**
Autoridad Nacional de Comunicación, Ghana
- **Dr Wolfgang Balzer**
Director General, Focus Infocom, Alemania

25 de noviembre de 2020

<p>09:00 – 09:30</p>	<p>Visión general y resultados del Grupo de Trabajo de Seguridad, Infraestructura y Confianza de FIGI</p> <p>Panelista</p> <ul style="list-style-type: none">• Vijay Mauree Coordinador de Programa, Oficina de Normalización de las Telecomunicaciones, ITU
<p>09:30 – 10:45</p>	<p>MARCO DE GARANTÍA DE SEGURIDAD: Gestión de Riesgos en los Servicios Financieros Digitales</p> <p>Los proveedores de DFS deben establecer medidas adecuadas para manejar las amenazas y vulnerabilidades a la seguridad y demostrar el cumplimiento frente a las medidas reglamentarias. En esta sesión se tendrán en cuenta las diversas amenazas y vulnerabilidades que pueden afectar la confidencialidad, integridad y disponibilidad de los servicios financieros digitales desde una perspectiva de la cadena de valor. La sesión también destacará las medidas de mitigación que los proveedores de DFS pueden implementar para reducir el impacto de los riesgos y debatir sobre un marco que pueden implementar los proveedores de DFS para administrar mejor los riesgos y demostrar el cumplimiento regulatorio.</p> <p>Moderador: Vijay Mauree, ITU</p> <p>Panelistas</p> <ul style="list-style-type: none">• Kevin Butler Universidad de Florida, "Marco de garantía de seguridad DFS"• Rehan Masood Banco Estatal de Pakistán, "Marco de seguridad de aplicaciones de pago"

11:00 – 12:00

SEGURIDAD DE LA INFRAESTRUCTURA: Protección de las aplicaciones e infraestructuras de DFS

Las vulnerabilidades SS7 pueden ser explotadas por intrusos para interceptar llamadas y mensajes SMS, evitar facturación en operaciones, robar dinero de cuentas móviles o afectar las operaciones en la red móvil. Además, las vulnerabilidades en las aplicaciones DFS también pueden conducir a que los piratas informáticos puedan obtener acceso no autorizado a los datos del consumidor si no se abordan correctamente. En esta sesión se presentarán las conclusiones del Grupo de Trabajo de Seguridad, Infraestructura y Confianza para proteger de vulnerabilidades y amenazas a la infraestructura a los servicios DFS (es decir, las vulnerabilidades del SS7) y el trabajo que se está llevando a cabo en la Comisión de Estudio 11 de la UIT-T y otros consorcios en la industria.

Moderador: Vijay Mauree, ITU

Panelistas

- **Assaf Klinger**
Klinger Consulting
- **Cathal Mc Daid**
CTO, Adaptive Mobile

26 de noviembre de 2020

9:00 – 10:40

Implementación de ID descentralizado para la autenticación e incorporación en finanzas digitales.

La identidad descentralizada está surgiendo como una tecnología clave para satisfacer la demanda de un medio eficaz para integrar a los clientes de una manera segura. Muchas de las soluciones descentralizadas suponen que el usuario es participante activo en la administración de sus identidades en línea. Estos usuarios comienzan con una identidad autoafirmada que gradualmente se puede actualizar por medio de sus relaciones. Por otro lado, algunas otras soluciones programan la autenticación de la identidad del usuario desde la primera interacción con pretensiones de confianza de la identidad. En esta sesión se examinarán los beneficios principales que se obtienen mediante el uso de DLT para la verificación de identidad y la autenticación, incluyendo el uso de GADI como conducto para la investigación y autenticación de identidad de confianza.

Moderator: Abbie Barbir, Comisión de Estudio 17, ITU-T

Panelistas

- **Jason Burnett**
DID Alliance “Visión general de GADI y casos de uso para finanzas digitales”
- **Kiran Adepalli**
Digital Trust “GADI – Referencia de implementación”
- **Matthew Davie**
“Implementación de ID Digital en Sierra Leona”

10:45 – 12:00

Autenticación segura mediante Fast Identity Online (FIDO)

Esta sesión proporciona una visión general de las tecnologías actuales para eliminar el uso de contraseñas en las transacciones digitales. Se presentan los riesgos de seguridad de las contraseñas y una visión general de cómo la tecnología FIDO ataca las limitaciones de seguridad en las contraseñas. La sesión se centrará en las últimas adiciones al protocolo FIDO, en particular WebAuthN, así como la compatibilidad con exploradores para el protocolo. El estado de soporte de FIDO en varios navegadores está cubierto, incluyendo soluciones mínimas viables que aseguran la interoperabilidad.

Moderator: Abbie Barbir, Comisión de Estudio 17, ITU-T

Panelistas

- **Cisa, Kurian,**
CVS "Lecciones aprendidas de la implementación de *WebAuth*"
- **Arnold Kibuuka,**
ITU "Visión general del despliegue actual de UIT FIDO"