|  |  |  |  |
| --- | --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | | **Unión Internacional de Telecomunicaciones**  **Oficina de Normalización de las Telecomunicaciones** | |
|  |  | | Ginebra, 25 de febrero de 2022 |
| **Ref.:** | **Circular TSB 382** TSB Events/VM | | – A las Administraciones de los Estados Miembros de la Unión;  – A los Miembros de Sector del UIT-T;  – A los Asociados del UIT-T;  – A las Instituciones Académicas de la UIT  **Copia**:  – A los Presidentes y Vicepresidentes de las Comisiones de Estudio;  – A la Directora de la Oficina de Desarrollo de las Telecomunicaciones;  – Al Director de la Oficina de Radiocomunicaciones  – A los Directores de las Oficinas Regionales de la UIT |
| **Contacto:** | **Vijay Mauree** | |
| **Tel.:** | +41 22 730 5591 | |
| **Fax:**  **Correo-e:** | +41 22 730 5853  tsbevents@itu.int | |
| **Asunto:** | **Taller Práctico sobre Seguridad de los SFD: Afrontar los riesgos de seguridad en el ecosistema financiero digital**  **(Plenamente virtual, 30 y 31 de marzo de 2022)** | | |

Muy Señora mía/Muy Señor mío:

1 Me permito comunicarle que la Unión Internacional de Telecomunicaciones organizará un Taller Práctico sobre Seguridad de los Servicios Financieros Digitales (SFD) en colaboración con la Organización de Comunicaciones de África Oriental (EACO) los días 30 y 31 de marzo de 2022 titulado "**Afrontar los riesgos de seguridad en el ecosistema financiero digital**".

2 El objetivo principal del Taller Práctico sobre Seguridad de los SFD es compartir las conclusiones y recomendaciones del [Grupo de Trabajo sobre seguridad, infraestructura y confianza de la Iniciativa Mundial de Inclusión Financiera (FIGI)](https://www.itu.int/en/ITU-T/extcoop/figisymposium/Pages/FIGISITWG.aspx) dirigidas a los organismos reguladores y los proveedores de SFD con respecto a la forma de afrontar los problemas de seguridad de las finanzas digitales. En este taller se proporcionará información sobre las mejores prácticas de seguridad para los intercambios de tarjetas SIM, las aplicaciones de pago móvil basadas en USSD, STK y Android, la metodología para probar la seguridad de las aplicaciones de pago móvil y afrontar las vulnerabilidades de infraestructura, como el SS7. En el Anexo 1 figura un proyecto de programa del Taller Práctico sobre Seguridad.

3 En el marco del programa de la FIGI, la UIT creó en noviembre de 2020 un Laboratorio de Seguridad de los SFD para trabajar en colaboración con los organismos reguladores de los SFD en la adopción de una metodología común para gestionar los riesgos de seguridad y realizar auditorías de seguridad de las aplicaciones de SFD. Los objetivos del Laboratorio de Seguridad de los SFD de la UIT son los siguientes:

a) Prestar apoyo a los organismos reguladores para que apliquen las recomendaciones de seguridad de la FIGI para los SFD (<https://figi.itu.int/working-group-reports/>).

b) Realizar auditorías de seguridad en aplicaciones de SFD (a saber, aplicaciones de SFD basadas en USSD, STK y Android).

c) Proporcionar orientación sobre la gestión de los riesgos de seguridad del ecosistema de los SFD y las correspondientes medidas de mitigación.

d) Organizar talleres prácticos sobre seguridad dirigidos a los organismos reguladores y a los proveedores de SFD para que se mantengan al día respecto de las nuevas vulnerabilidades y las medidas de mitigación.

e) Llevar a cabo evaluaciones de la ciberpreparación entre las partes interesadas del ecosistema de los SFD a la hora de responder a los incidentes de ciberseguridad dirigidos contra las finanzas digitales.

f) Proporcionar una plataforma neutral para compartir conocimientos sobre incidentes de seguridad y vulnerabilidades en las finanzas digitales.

4 El Taller Práctico sobre Seguridad de los SFD está dirigido a los profesionales en materia de seguridad informática y a los encargados de la formulación de políticas de los organismos reguladores de las telecomunicaciones/TIC, los proveedores de SFD, los bancos centrales y los operadores de redes móviles.

5 Toda la información pertinente relativa a este taller (oradores, enlace de inscripción, detalles de la conexión a distancia) estará disponible en la página web del evento en la siguiente dirección: <https://www.itu.int/en/ITU-T/webinars/dfs/sc/20220330/Pages/default.aspx>.

Rogamos tenga presente que la inscripción es obligatoria.

Atentamente

A picture containing logo

Description automatically generatedChaesub Lee  
Director de la Oficina de   
Normalización de las Telecomunicaciones

Anexo 1: Proyecto de programa del Taller Práctico sobre Seguridad de los SFD: *Afrontar los riesgos de seguridad en el ecosistema financiero digital*

|  |  |
| --- | --- |
| Primer día: 30 de marzo de 2022, 10.00-13.00 horas (hora de África oriental) | |
| 10.00-10.20 | Apertura del taller y discurso de bienvenida  **• Bilel Jamoussi**, Jefe del Departamento de Comisiones de Estudio de la TSB, UIT  **• Ally Yahaya Simba,** Secretario Ejecutivo de la EACO |
| 10.20-11.50 | **Vulnerabilidades de seguridad de los SFD: Vulnerabilidades de infraestructura y medidas de mitigación (vulnerabilidades de la infraestructura móvil)**  Las vulnerabilidades de la infraestructura de telecomunicaciones, como el SS7, pueden ser aprovechadas por un intruso para interceptar llamadas y SMS, eludir el pago de facturas, robar dinero de las cuentas de dinero móvil o afectar a las operaciones de la red móvil. En esta sesión se presentarán las principales conclusiones del Grupo de Trabajo sobre seguridad, infraestructura y confianza en materia de protección de la infraestructura contra las vulnerabilidades y amenazas del SS7.  **Oradores**  • "Seguridad de la señalización" – **Faaez Burney** y **Karel Van Der Lecq**, Adaptive Mobile  • "Seguridad del SS7: ¿Qué deben hacer los organismos reguladores?" – **Assaf Klinger**, Klinger Consulting  Informe relacionado:  • [SS7 Vulnerabilities and Mitigation Measures for DFS Transactions](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) (Vulnerabilidades del SS7 y medidas de mitigación para las transacciones de SFD) |
| 11.50-12.00 | **Descanso** |
| 12.00-13.00 | **Vulnerabilidades de seguridad de los SFD: Vulnerabilidades de las plataformas basadas en USSD, STK y Android**  En esta sesión se presentará el Laboratorio de Seguridad de los SFD de la UIT y se destacarán las vulnerabilidades de las aplicaciones basadas en USSD, STK y Android. Se examinarán amenazas como los ataques por intermediario, que podrían afectar a los servicios financieros digitales, y la vulnerabilidad "SIMjacker" de las tarjetas SIM. En la sesión se realizará además una presentación general de las pruebas de seguridad que pueden llevarse a cabo en el Laboratorio de Seguridad de los SFD de la UIT.  **Oradores**  • "Presentación del Laboratorio de Seguridad de los SFD" – **Vijay Mauree**, Coordinador de Programas de la TSB, UIT  • "Pruebas de Android, USSD y STK" – **Arnold Kibuuka**, Administrador de Proyectos de la TSB, UIT  Informes relacionados:  • [Security testing for USSD and STK based DFS applications](https://figi.itu.int/wp-content/uploads/2021/04/Security-testing-for-USSD-and-STK-based-Digital-Financial-Services-applications-1.pdf) (Pruebas de seguridad para aplicaciones de SFD basadas en USSD y STK)  • [Security audit of various DFS applications](https://figi.itu.int/wp-content/uploads/2021/05/Security-audit-of-various-DFS-applications.pdf) (Auditoría de seguridad de varias aplicaciones de SFD) |
| Segundo día: 31 de marzo de 2022, 10.00 – 13.00 horas (hora de África oriental) | |
| 10.00-11.15 | **Marco de garantía de seguridad de los SFD**  En esta sesión se examinará el marco de garantía de seguridad de los servicios financieros digitales que pueden aplicar los proveedores de dichos servicios para mejorar la gestión de los riesgos y mitigar sus repercusiones.  *•* **Vijay Mauree***,* Coordinador de Programas de la TSB, UIT  Informe relacionado:  • [DFS Security Assurance Framework](https://figi.itu.int/wp-content/uploads/2021/04/Technical-report-on-Digital-Financial-Services-Security-Assurance-Framework_f-1-1.pdf) (Marco de garantía de seguridad de los SFD) |
| 11.15-11.25 | **Descanso** |
| 11.25-12.00 | **Guía de auditoría de la seguridad de los SFD**  En esta sesión se examinará la manera en que un organismo regulador o proveedor de SFD puede evaluar el cumplimiento de los controles mínimos de seguridad utilizando la guía de auditoría de los SFD.  **• Arnold Kibuuka**, Administrador de Proyectos de la TSB, UIT  Informe relacionado:  • [DFS security audit guideline](https://figi.itu.int/wp-content/uploads/2021/05/Digital-Financial-Services-security-audit-guideline.pdf) (Guía de auditoría de la seguridad de los SFD) |
| 12.00-13.00 | **Aplicación de las recomendaciones y auditorías de seguridad de los SFD**  Esta sesión interactiva se centra en la puesta en marcha del proceso de aplicación de las recomendaciones de seguridad de los SFD y en la identificación de las aplicaciones de dinero móvil de los SFD que podrían someterse a pruebas en el Laboratorio de Seguridad de los SFD de la UIT. |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_