**ADD** AFCP/19A3/6

# AFR3: Creación de confianza y seguridad en la utilización de las telecomunicaciones/TIC

**Objetivo:** Ayudar a los Estados Miembros en la elaboración y aplicación de políticas, estrategias, normas y mecanismos que permitan mejorar la seguridad de los sistemas y redes de información, garantizar la interoperatividad de las tecnologías digitales, proteger los datos y a las personas, y afianzar la confianza digital. Proteger la infraestructura de TIC y crear confianza en la utilización de las TIC y sus aplicaciones.

Resultados previstos

1) Cumplimiento del objetivo de la Agenda Conectar 2020, en virtud del cual la preparación para la ciberseguridad debería haber mejorado un 40% en 2020.

2) Asistencia a los Estados Miembros en la evaluación y adaptación de los marcos legislativos y reglamentarios sobre la base de una mejor utilización del informe relativo al índice de ciberseguridad mundial de la UIT.

3) Promoción del desarrollo de un marco mundial de colaboración y sensibilización a nivel regional y subregional con miras a desarrollar una cultura global de ciberseguridad y ayudar a los consumidores a entender mejor los riesgos existentes y protegerse contra ellos.

4) Asistencia en la mejora de la formación de los consumidores en materia de cibercomercio y transacciones móviles, así como de sus conocimientos sobre la legislación financiera de las transacciones electrónicas y los sistemas de pago móvil.

5) Promoción del establecimiento de mecanismos institucionales y organizativos en los planos nacional y regional para facilitar la aplicación efectiva de las estrategias de ciberseguridad.

6) Elaboración de medidas tendentes a la protección de los consumidores, los niños y otras personas vulnerables al utilizar las TIC.

7) Creación de conciencia en torno a las ciberamenazas, las medidas de ciberseguridad y la calidad del servicio en el marco de la utilización de las TIC.

8) Adopción de medidas orientadas a la protección de la privacidad y los datos personales.

9) Asistencia en el establecimiento de estructuras adecuadas (centros de datos, puntos de intercambio Internet, etc.) para el desarrollo de la ciberseguridad y la lucha contra la ciberdelincuencia, y fomento de la creación deequipos de intervención en caso de incidente informático (EIII) a escala nacional y regional.

10) Formulación de una estrategia armonizada para mejorar la seguridad de la información y contrarrestar el correo basura y las ciberamenazas.