Documentos de referencia de la UIT

UIT: CREAR CONFIANZA EN LAS TIC Y EL CIBERESPACIO

La GCA facilita los esfuerzos de la UIT en la construcción de la capacidad tecnológica necesaria para ayudar a los países a combatir las ciberamenazas, recomendar normas globales sobre ciberseguridad y tecnología, y actuar como plataforma de conocimiento y de discusión pública de políticas.

La UIT prevé que cerca de 3.000 millones de personas utilizarán Internet a finales de 2014, abriéndose nuevas y atractivas posibilidades de acceso a la información y la comunicación. Al mismo tiempo, sin embargo, problemas de seguridad y vulnerabilidad en las redes y los servicios exponen permanentemente a los usuarios a ciberamenazas cada vez más sofisticadas. El robo de identidades, el correo basura, los programas maliciosos, la explotación y el abuso de niños y otros grupos de riesgo pueden tener consecuencias dramáticas, a veces devastadoras, en el mundo real, más allá de los 400.000 millones de dólares de pérdidas estimadas de la economía global.[1]

Como las tecnologías de la información y la comunicación (TIC) se han convertido en una infraestructura nacional crítica, sus perturbaciones pueden significar interrupciones catastróficas de servicios esenciales. Y en el entorno de la tecnología de banda ancha con conexión permanente, en cualquier lugar y en cualquier momento, los ataques se pueden producir en un país –o incluso en varios países simultáneamente– mientras que su autor puede estar en otro totalmente diferente.

Las ciberamenazas han aparecido como un riesgo para todos los países, incluso los más avanzados técnicamente. Una cooperación internacional más amplia puede ayudar a reducir este riesgo.

UNA AMENAZA INTERNACIONAL CRECIENTE

- Hubo casi 400 millones de víctimas de ciberamenazas en 2013.
- En 2013 se incrementaron un 91% las campañas de ataques dirigidos. El número de fallos de seguridad aumentó un 62% y un 38% de los usuarios de móviles sufrieron ciberdelitos.
- El número de 'identidades expuestas' se disparó, multiplicándose por más de cinco hasta alcanzar 552 millones en 2013, comparado con 93 millones en 2012.
- Los tres sectores de mayor riesgo frente a ataques dirigidos son gobierno, minería y fabricación (Symantec, 2014 Internet Security Threat Report).

Los usuarios de móviles a menudo almacenan ficheros sensibles en línea (52%), e información de trabajo y personal en la misma cuenta de almacenamiento en línea (24%), y frecuentemente comparten sus identificadores y palabras clave con familiares (21%) y amigos (18%), poniendo en riesgo sus datos y los de sus empresas. Sólo el 50% de los usuarios toma medidas básicas de seguridad, de acuerdo con Symantec, empresa asociada de la UIT.

1. *MacAfee*

La iniciativa de la UIT Protección de la Infancia en Línea (PleL) es una red de colaboración internacional diseñada para identificar los riesgos y las vulnerabilidades de los niños en el ciberespacio en todo el mundo, sensibilizar, compartir los recursos, elaborar herramientas para ayudar a reducir el riesgo y promover una ciudadanía digital responsable.

A medida que 'Internet de las Cosas' se convierte en una realidad, con millones de dispositivos conectados intercambiando información máquina a máquina sin necesidad de intervención humana, nuestros mundos reales y cibernéticos se están superponiendo cada vez más. La UIT está en primera línea, agrupando a las diferentes partes interesadas en asociaciones globales, a la hora de ofrecer soluciones técnicas y políticas para combatir los problemas de la ciberseguridad.

Una evolución fundamental ha sido la creación de la Agenda sobre Ciberseguridad Global (GCA) de la UIT, que es un marco internacional para la cooperación. La GCA facilita los esfuerzos de la UIT en la construcción de la capacidad tecnológica necesaria para ayudar a los países a combatir las ciberamenazas, recomendar normas globales sobre ciberseguridad y tecnología, y actuar como plataforma de conocimiento y de discusión pública de políticas.

Responder a los ciberataques nacionales

Un ciberataque a nivel nacional puede causar estragos en las infraestructuras críticas y tener repercusiones directas sobre muestra vida diaria; desde no poder acceder a nuestra cuenta bancaria hasta provocar la interrupción del transporte público, la interrupción del suministro eléctrico, el bloqueo de las comunicaciones o consecuencias peores.

Existe una clara necesidad de que las instituciones afronten los ciberincidentes y ataques. La UIT trabaja con los Estados Miembros, las regiones y los asociados de la industria para poder desplegar y construir esta capacidad, a nivel nacional y regional.

La UIT crea la capacidad y el conocimiento realizando amplios programas de capacitación y apoyo. Entre estas iniciativas se encuentran las siguientes:

- Asistir a 50 Estados Miembros para llevar a cabo evaluaciones de su preparación en ciberseguridad y su capacidad de respuesta a nivel nacional. Siete Estados Miembros han recibido apoyo para crear equipos de intervención en caso de incidentes informáticos (CIRT), y siete más confirmaron su necesidad de apoyo a la UIT.

- Hasta la fecha, se han realizado siete ciberejercicios CIRT con más de 60 países participantes. Estos ejercicios evalúan si las funciones clave de los CIRT establecidos son coherentes con las normas internacionales y las buenas prácticas.

- El establecimiento de estrategias nacionales de ciberseguridad es un reto, en particular para los Países Menos Adelantados (PMA) que carecen de los marcos jurídicos y reglamentarios adecuados, tienen conocimientos y capacidad limitados, y les falta recursos financieros para identificar, gestionar y responder a las ciberamenazas. El proyecto de la UIT "Mejora de la ciberseguridad en los países menos adelantados" ayuda a los PMA a reforzar sus capacidades en ciberseguridad para asegurar una mejor protección de sus infraestructuras nacionales y maximizar los beneficios socio-económicos.

- A nivel regional, se proporciona una asistencia adicional en forma de Centros de Ciberseguridad Regionales de la UIT – un centro físico albergado por un Estado Miembro que actúa como el punto focal de la UIT a nivel regional para temas de ciberseguridad. El Centro Regional de Ciberseguridad árabe está ubicado en Omán y existen planes para la construcción de un Centro Regional de Ciberseguridad africano en Nigeria.

- La UIT ayuda los Estados Miembros a entender los aspectos legales de la ciberseguridad, para armonizar sus marcos jurídicos con el objetivo de que sean aplicables y puedan interfuncionar en todo el mundo.

- El creciente papel que juegan las TIC en la prestación de servicios en sectores tan variados como la sanidad, la educación, las finanzas y el comercio subraya la necesidad de tener un ciberentorno globalmente seguro. No obstante, existe actualmente una escasez de profesionales cualificados en ciberseguridad en todos los países. Para ayudar a cerrar esta brecha, la UIT ha organizado talleres de capacitación en ciberseguridad para más de 1.900 funcionarios, reguladores, y profesionales del sector público y privado de las TIC en todo el mundo.

La seguridad es un elemento fundamental en las recomendaciones y normas de la UIT, y todas las Comisiones de Estudio de la UIT revisan de manera regular las cuestiones relacionadas con la seguridad como parte de su trabajo.

Protección de la Infancia en Línea (PIeL)

Los niños son uno de los grupos más vulnerables en línea; la generación de 'nativos digitales' es mucho más propensa a revelar datos personales en línea convirtiéndose en objetivo fácil de los delincuentes y de los piratas (hackers).

La separación entre el mundo real y el mundo en línea está siendo cada vez más porosa – con consecuencias serias para la salud mental y física de un niño. En un estudio reciente, casi la mitad de los adolescentes de 13 a 17 años indicaron que habían sufrido algún tipo de ciberacoso durante el año anterior. E incluso más preocupante, tres de cada cuatro jóvenes que sufrieron casos de agresión sexual en la vida real habían conocido a sus agresores en línea.

La iniciativa de la UIT Protección de la Infancia en Línea (PIeL) es una red de colaboración internacional diseñada para identificar los riesgos y las vulnerabilidades de los niños en el ciberespacio en todo el mundo, sensibilizar, compartir los recursos, elaborar herramientas para ayudar a reducir el riesgo y promover una ciudadanía digital responsable. En el ámbito de la iniciativa PIeL, más de 54 asociados internacionales de gobiernos, el sector privado, la sociedad civil, instituciones académicas y organizaciones internacionales trabajan juntos para conseguir estos objetivos.

Normas técnicas (Recomendaciones)

Las normas técnicas de la UIT (conocidas como Recomendaciones) tienen un papel fundamental en la protección de los usuarios en línea. La Comisión de Estudio 17 del UIT-T es la Comisión de Estudios Rectora para asuntos de seguridad y gestión de la identidad, y se centra fundamentalmente en la creación de confianza y seguridad en la utilización de las TIC.

La seguridad es un elemento fundamental en las recomendaciones y normas de la UIT, y todas las Comisiones de Estudio de la UIT revisan de manera regular las cuestiones relacionadas con la seguridad como parte de su trabajo. Los logros a fecha de hoy incluyen: Recomendaciones técnicas para redes basadas en el Protocolo Internet (IP), Normas para las Redes de la Próxima generación (NGN) y asegurar unos principios claros de seguridad en las redes celulares móviles de hoy y de mañana. Un ejemplo destacado es la **X.509**, una Recomendación del UIT-T sobre la infraestructura de clave pública (PKI y la infraestructura de gestión de privilegios (PMI). La Rec. X.509 especifica, entre otras cosas, los formatos normalizados para certificados de clave pública, las listas de revocación de certificados y los certificados de atributos.

Una aproximación global, con todas las partes interesadas

- La ciberseguridad es una prioridad cada vez mayor, debido a la dependencia cada vez mayor de los Países Menos Adelantados (PMA) en las TIC y con estudios que indican que los países en desarrollo son los más vulnerables a los ciberdelitos y ciberamenazas. El proyecto de la UIT "Mejora de la ciberseguridad en países menos adelantados" tiene por objeto proteger a los usuarios y hacer Internet más segura a través de la asistencia a nivel político.

- La UIT se ha asociado con ABI Research para el Índice Mundial de Ciberseguridad (GCI) a fin de evaluar el grado de desarrollo de la ciberseguridad en cada país y permitir que los Estados Miembros aprendan de las mejores prácticas.

- La UIT ha establecido también una cooperación formal con empresas de ciberseguridad, como Symantec y Trend Micro, para compartir regularmente información sobre las tendencias, actuales y futuras, de las ciberamenzas globales.

- La UIT trabaja actualmente con otros organismos/agencias de Naciones Unidas para mejorar la coordinación entre estos organismos en su apoyo a los Estados Miembros en los aspectos de ciberseguridad.