ITU Publicaciones
Periodo de estudios 2018-2021

Unión Internacional de Telecomunicaciones
Sector de Desarrollo

Comisión de Estudio 2 Cuestión 3

Seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad

Informe de resultados sobre la

Cuestión 3/2 del UIT-D

Seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad

Periodo de estudios 2018-2021

Seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad: Informe de resultados sobre la Cuestión 3/2 del UIT-D para el periodo de estudios 2018-2021

ISBN 978-92-61-34103-9 (versión electrónica)
ISBN 978-92-61-34113-8 (versión EPUB)
ISBN 978-92-61-34123-7 (versión Mobi)

Cita recomendada: Seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad: Informe de resultados sobre la Cuestión 3/2 del UIT-D para el periodo de estudios 2018-2021. Ginebra: Unión Internacional de Telecomunicaciones, 2021. Licencia: CC BY-NC-SA 3.0 IGO.

Fotografía de la portada: Shutterstock

Agradecimientos

Las Comisiones de Estudio del Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D) brindan una plataforma neutral en la que expertos de gobiernos, empresas, organizaciones de telecomunicaciones e instituciones académicas de todo el mundo pueden reunirse y crear herramientas y recursos prácticos para abordar cuestiones de desarrollo. A tal efecto, las dos Comisiones de Estudio del UIT-D se encargan de elaborar Informes, Directrices y Recomendaciones partiendo de las contribuciones recibidas de los Miembros. Las Cuestiones de estudio se determinan cada cuatro años en el marco de la Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT). Los miembros de la UIT, reunidos en la CMDT-17, que se celebró en Buenos Aires en octubre de 2017, decidieron que la Comisión de Estudio 2 se ocupara de siete Cuestiones relacionadas con los "servicios y aplicaciones de las tecnologías de la información y la comunicación en pro del desarrollo sostenible" durante el periodo de estudios 2018-2021.

El presente informe se preparó en respuesta a la Cuestión 3/2: **Seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad**, bajo la dirección y coordinación generales del equipo directivo de la Comisión de Estudio 2 del UIT-D, encabezado por el Sr. Ahmad Reza Sharafat (República Islámica del Irán), en calidad de Presidente, con el apoyo de los siguientes Vicepresidentes: Sr. Nasser Al Marzouqi (Emiratos Árabes Unidos)(dimitió en 2018); Sr. Abdelaziz Alzarooni (Emiratos Árabes Unidos); Sr. Filipe Miguel Antunes Batista (Portugal)(dimitió en 2019); Sra. Nora Abdalla Hassan Basher (Sudán); Sra. Maria Bolshakova (Federación de Rusia); Sra. Celina Delgado Castellón (Nicaragua); Sr. Yakov Gass (Federación de Rusia)(dimitió en 2020); Sr. Ananda Raj Khanal (República de Nepal); Sr. Roland Yaw Kudozia (Ghana); Sr. Tolibjon Oltinovich Mirzakulov (Uzbekistán); Sra. Alina Modan (Rumania); Sr. Henry Chukwudumeme Nkemadu (Nigeria); Sra. Ke Wang (China); y Sr. Dominique Würges (Francia).

El informe se elaboró bajo la dirección de los Correlatores para la Cuestión 3/2, el Sr. Michael Beirne (Estados Unidos)(dimitió en 2020); el Sr. Kwadwo Burgee (Estados Unidos)(dimitió en 2020); la Sra. Aimee K. Meacham (Estados Unidos); y el Sr. Dominique Würges (Francia), en colaboración con los siguientes Vicerrelatores: Sr. Damnam Kanlanfei Bagolibe (Togo); Sr. Amine Adoum Bakhit (Chad); Sra. Maria Bolshakova (Federación de Rusia); Sra. Sonam Choki (Bhután); Sr. Yakov Gass (Federación de Rusia)(dimitió en 2020); Sr. Karim Hasnaou (Argelia); Sr. Cissé Kane (Sociedad Civil Africana sobre la Sociedad de la Información); Sra. Miho Naganuma (Japón); Sr. Jean-David Rodney (Haití); Sra. Jabin Vahora (Estados Unidos); Sra. Xinxin Wan (China); Sr. Jaesuk Yun (República de Corea); y Sr. Mohamadou Zarou (Malí).

Merecen un agradecimiento especial los coordinadores de los capítulos por su dedicación, su apoyo y su competencia.

El presente informe se ha elaborado con el apoyo de los coordinadores de la BDT, los editores, el equipo de producción de publicaciones y la secretaría de las Comisiones de Estudio del UIT-D.

Índice

Lista de cuadros y figuras

Cuadros

Figuras

Resumen ejecutivo

El objetivo de la Cuestión 3/2 ("Seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad") es preparar informes sobre prácticas idóneas relativas a diversos aspectos de la ciberseguridad.

En este documento se presenta el Informe final de la Cuestión 3/2 para el último periodo de estudios de cuatro años (2018-2021) cuyo programa de trabajo fue creado por la Conferencia Mundial de Desarrollo de las Telecomunicaciones en su reunión de 2017 celebrada en Buenos Aires (CMDT-17).

En los periodos de estudio anteriores las actividades se centraron en el material didáctico disponible (2010-2014) y en talleres destinados a aportar un amplio conjunto de actores y contenidos a los países en desarrollo (2014-2017).

A lo largo del periodo de estudios 2018-2021 la Comisión de Estudio 2 del UIT-D abordó la mayoría de temas de su programa de trabajo. También en este periodo de estudio se celebró un taller.

Este Informe de la Cuestión 3/2 se basa en el material presentado por los miembros de la UIT en sus contribuciones a lo largo del periodo de estudio. El informe describe el panorama general de los mensajes basura (*spam*) y de los programas maliciosos (*malware*), así como los mecanismos para hacerles frente. Contiene, además, una serie de lecciones para la planificación de la respuesta nacional en materia de ciberseguridad y las campañas de sensibilización. Asimismo, incluye lecciones sobre medidas particulares para las personas vulnerables, incluidas las personas con discapacidad y los niños. Por añadidura, el informe contiene lecciones sobre ciudades inteligentes, tecnologías emergentes y protección de datos.

En el actual mundo digitalizado, la vida cotidiana de los ciudadanos y las economías dependen cada vez más de las tecnologías digitales, por lo que existe un mayor riesgo de vulnerabilidad y de estar más expuesto a los ciberataques. La ciberseguridad se ha convertido en una prioridad y es uno de los aspectos que suscita mayor preocupación de la industria, los gobiernos y los usuarios de Internet en todo el mundo, y además resulta fundamental para el progreso en condiciones de seguridad que permita el crecimiento de la sociedad.

El presente informe tiene por objeto aportar ideas y prácticas renovadas basadas en la experiencia de los miembros de la UIT. Habida cuenta de que el entorno general y el panorama de las amenazas no dejan de evolucionar, el informe pretende ser simplemente una radiografía actual de este ámbito tan sensible como es el de la ciberseguridad. Este informe también se publica en un contexto muy específico y hasta ahora desconocido: pese a que no hay referencias específicas a la pandemia actual, las consecuencias de la COVID-19 estuvieron presentes en la mente de muchos contribuyentes y en los debates durante las actividades de la Cuestión 3/2.

Las respuestas y propuestas recopiladas en este informe tienen por objeto ayudar a conseguir un elevado nivel de ciberseguridad en todos los miembros de la UIT, y quizá también puedan servir como herramienta útil para posibles crisis futuras, que se sumen a las demás acciones emprendidas por la UIT.

En el **Capítulo 1** se ofrece información actualizada sobre la situación de los mensajes basura y los programas maliciosos y sobre cómo reaccionar para su atenuación. Obsérvese que la Comisión de Estudio no recibió contribuciones directas sobre este tema.

En el **Capítulo 2** se describe cómo mejorar la postura nacional en materia de ciberseguridad mediante la sensibilización y la capacitación.

En el **Capítulo 3** se aborda el tema de la protección de la infancia en línea (PIeL).

En el **Capítulo 4** se examinan los problemas de ciberseguridad específicos de las personas con discapacidad.

En el **Capítulo 5** se analizan los problemas de ciberseguridad para las tecnologías incipientes, como Internet de las cosas (IoT) y la computación en la nube.

En el **Capítulo 6** se presentan diferentes perspectivas sobre cómo puede contribuir la ciberseguridad a la protección de los datos personales.

Por último, en el **Capítulo 7** se tratan las futuras esferas de estudio.

Además de este informe, cabe señalar que la Cuestión 3/2 revisó el cuestionario que sirve de base para el Índice de Ciberseguridad Global (ICG) y formuló sus comentarios y propuestas al respecto, lo que permitió a la BDT realizar su encuesta anual a los Estados Miembros de la UIT. Concretamente, por iniciativa de Brasil, la Cuestión 3/2 preparó la encuesta que se incorporó como anexo al ICG. Las revisiones propuestas se integraron en la cuarta edición del ICG 2020.

Este Informe no se detiene en el ICG, aunque la Cuestión 3/2 destaca lo positivo del esfuerzo colectivo y de la fructífera colaboración con la BDT, pues las respuestas a dicho anexo ofrecerán información sobre políticas reglamentarias que la BDT pondrá a disposición de sus miembros, cumpliendo así el punto "n" del mandato de la Cuestión 3/2.

Capítulo 1 – Información actualizada sobre la situación de los mensajes basura y los programas maliciosos, con inclusión de las respuestas de mitigación

En esta sección se examina la evolución de los mensajes basura y los programas maliciosos y se exponen una serie de medidas para contrarrestarlos a nivel nacional, regional e internacional, de conformidad con la Resolución 45 (Rev. Dubái, 2014) de la conferencia Mundial de Desarrollo de las Telecomunicaciones[1], sobre los mecanismos para mejorar la cooperación en materia de ciberseguridad, incluida la lucha contra los mensajes basura. Esta sección responde así a los apartados 2 b) y m) del mandato de la Cuestión 3/2 que figura en el Informe final de la CMDT-17:

b) considerar enfoques y mejores prácticas para evaluar el impacto del correo basura y de los programas informáticos dañinos dentro de una red, así como la evolución de nuevas amenazas, y ofrecer los insumos necesarios con miras a la elaboración de medidas y directrices, tales como técnicas de mitigación, aspectos legislativos y normativos que los países puedan utilizar, teniendo en cuenta las normas existentes y las herramientas disponibles;

m) proporcionar orientaciones sobre medidas que permitan hacer frente al correo basura y los programas informáticos dañinos a escalas nacional, regional e internacional[2].

1.1 Situación de los mensajes basura y de los programas maliciosos

Si bien no existe una definición de mensajes basura (*spam*) universalmente aceptada, en general se refiere a las comunicaciones electrónicas masivas no solicitadas que se envían a través de ordenadores o teléfonos móviles mediante correo electrónico y mensajes de texto.[3] Los consumidores suelen percibir que los mensajes basura son publicidad, incluyendo correos electrónicos comerciales no deseados, textos y contactos en las redes sociales.

Aunque los mensajes basura suelen ser una forma de promoción comercial, en ocasiones también utiliza datos similares generados por los usuarios con fines delictivos, como la *peska* o *phishing*. Haciéndose pasar por un tercero de confianza, los delincuentes utilizan los correos electrónicos de *peska* para instar a los destinatarios a revelar datos personales (cuentas de acceso, contraseñas, etc.) y/o datos bancarios.

Los mensajes basura suponen un riesgo para la seguridad de los usuarios y las organizaciones conectadas, no solo porque se difunden fácilmente a través de Internet y los servicios de

1 UIT. Informe final de la Conferencia Mundial de Desarrollo de las Telecomunicaciones (Buenos Aires, 2017), p. 409.
2 *Ibid*. pp. 727-728.
3 Véanse las Recomendaciones UIT-T X.1230 a UIT-T X.1240 sobre la lucha contra los mensajes basura.

comunicación electrónica (correo electrónico, sitios web, redes sociales, SMS y MMS), sino también porque pueden ser portadores de programas maliciosos. Los países están aplicando con cierto éxito diversos mecanismos técnicos y normativos para combatir los mensajes basura.

Los programas maliciosos, por su parte, han experimentado un fuerte crecimiento en los últimos años debido al desarrollo de Internet y, más concretamente, de Internet móvil. Se denomina programa malicioso al *software* diseñado específicamente para dañar computadores o sistemas informáticos.[4]

Por otra parte, el aumento de la conectividad, las nuevas tecnologías y el crecimiento del número de usuarios han brindado nuevas oportunidades para la creación y el uso de programas maliciosos. Este paradigma introduce una mayor complejidad para la ciberseguridad al abrir brechas y ampliar las superficies de ataque disponibles para las amenazas de los programas maliciosos. Además de los tradicionales (virus, gusanos, troyanos, programas espía, programas publicitarios, mensajes basura, rootkits, etc.), han surgido nuevos tipos de programas maliciosos más sofisticados, como las redes de bots, los programas de extorsión y los programas maliciosos para móviles.

En resumen, contrarrestar los mensajes basura y los programas maliciosos es fundamental para la seguridad de los usuarios y el crecimiento de las empresas.

1.2 Mensajes basura y programas maliciosos: estadísticas, tendencias, evolución e incidencia en las redes de comunicaciones electrónicas

Al mes de marzo de 2020, la proporción de mensajes basura en el tráfico mundial de correo electrónico era del 53,95 por ciento.[5] En los últimos años, este porcentaje ha disminuido considerablemente, pasando del 69 por ciento en 2012 al 55 por ciento en 2018, posiblemente como resultado de los progresos en materia de sensibilización sobre ciberseguridad y de los adelantos tecnológicos. La mayor parte de los correos basura que reciben los usuarios son de carácter publicitario, incluida información de comercialización. Según una estimación, ese tipo de mensajes cuesta a las empresas casi 20 500 millones USD cada año en pérdida de productividad y gastos técnicos. Se ha sugerido que, si el correo basura sigue creciendo al ritmo actual, este coste podría aumentar a 257 000 millones USD.[6]

Se calcula que las estafas y los fraudes representan alrededor del 2,5 por ciento de todos los mensajes basura, de los cuales una proporción significativa (92 por ciento) podría ser de origen malicioso, es decir, relacionado con programas maliciosos destinados a perjudicar a los usuarios o a comprometer sus sistemas informáticos con diversos fines.[7] Según otra estimación, en 2018 se identificaron alrededor de 812,67 millones de infecciones de diversos tipos relacionadas con los programas maliciosos.[8] Los programas maliciosos para móviles han aumentado en un 54 por ciento y los programas de extorsión en un 350 por ciento, mientras que las pérdidas financieras relacionadas con las infecciones por programas de extorsión se estiman en 6 000 millones USD al año (hasta 2021).

---

4 Véase el Suplemento 9 a la Recomendación UIT-T X.1205 (09/2011), Suplemento sobre directrices para reducir los programas informáticos malignos en las redes de TIC.
5 Statista. Global spam volume as percentage of total e-mail traffic from January 2014 to September 2020, by month.
6 Spam Laws. Spam statistics and facts.
7 DataProt. What's on the other side of your inbox – 20 SPAM statistics for 2021.
8 PurpleSec. 2021 Cyber Security Statistics – The Ultimate List of stats, data & trends.

Como los mensajes basura y los programas maliciosos pueden generar un volumen considerable de tráfico, tienen un efecto negativo importante en la infraestructura de la red y en los operadores y, por ende, en la experiencia de los usuarios. Los problemas relacionados con los mensajes basura, comprendidos los ocasionados a la red, también pueden menoscabar la reputación de los operadores.

Para hacer frente a estos problemas, en particular el flujo potencialmente masivo de tráfico no deseado, y garantizar la calidad de la red, es posible que los operadores tengan que desarrollar nuevas herramientas, como invertir en salvaguardias y ampliación de la infraestructura existente. Por ejemplo, los proveedores de servicios podrían invertir en filtros contra los mensajes basura para mejorar la calidad de los servicios que ofrecen. Esto puede suponer un coste necesario adicional para los operadores y los proveedores de servicios de comunicaciones electrónicas.

1.3 Medidas adoptadas para contrarrestar y mitigar los efectos de los mensajes basura y los programas maliciosos

1.3.1 Medidas técnicas para contrarrestar y mitigar los efectos de los mensajes basura y los programas maliciosos

El correo electrónico no solicitado es uno de los principales canales de transmisión de programas maliciosos. Para luchar eficazmente contra los mensajes basura y los programas maliciosos, hay que romper la cadena de transmisión. A medida que la tecnología ha ido avanzando, herramientas como los filtros *antispam* y los programas antivirus siguen siendo mecanismos eficaces para combatir los mensajes basura y los programas maliciosos. La eficacia de estas herramientas puede mejorarse si se utilizan junto con nuevas tecnologías, como la inteligencia artificial (IA). Actualizar regularmente los filtros *antispam* y los programas antivirus es, por tanto, una buena práctica para los usuarios.

Entre los proveedores de servicios, pueden utilizarse políticas como el convenio de remitentes (*Sender Policy Framework*[9]), el correo identificado por claves de dominio (*Domain Keys Identified Mail*[10]), la autentificación, notificación y conformidad de mensajes basada en el dominio (*Domain-based Message Authentication, Reporting and Conformance*[11]) y la inscripción en listas de bloqueo en tiempo real para reducir estas cadenas de transmisión.

Los operadores de redes de comunicaciones electrónicas y los proveedores de servicios de Internet también pueden adoptar ciertas medidas para resolver los problemas relacionados con el bloqueo de direcciones IP. Un ejemplo es la seguridad del Protocolo de pasarela limítrofe mediante la infraestructura de clave pública de recursos.[12] Otras iniciativas son:

- Normas mutuamente acordadas para la seguridad del encaminamiento, cuyo objetivo es evitar de manera colaborativa el secuestro de rutas, la suplantación de direcciones IP y otras actividades maliciosas que pueden dar lugar a ataques distribuidos de denegación de servicio (DDoS), escuchas, pérdida de ingresos, perjuicio para la reputación, etc.[13]
- Grupo de Trabajo contra el abuso en la mensajería, programas maliciosos y móviles, que publica periódicamente prácticas idóneas para combatir los mensajes abusivos, todos los

9 Mimecast. Everything you need to know about SPF.
10 DKIM.org. DomainKeys Identified Mail (DKIM).
11 DMARC. Autentificación, notificación y conformidad de mensajes basadas en el dominio.
12 RFC Editor. RFC 6480 – An Infrastructure to Support Secure Internet Routing, febrero de 2012.
13 MANRS. Normas mutuamente acordadas para la seguridad del encaminamiento.

tipos de programas maliciosos (redes de bots inclusive), mensajes basura, virus, ataques de denegación del servicio (DoS) y cualquier tipo de abuso en línea.[14]

Otras iniciativas contra los mensajes basura y los programas maliciosos son la Internet Society[15], la Asociación GSM (Global System for Mobile Communications)[16], el Proyecto Spamhaus[17], el Grupo de Trabajo Anti-Phishing[18] y la Anti-Spyware Coalition[19].

1.3.2 Ejemplos de medidas reglamentarias para contrarrestar y mitigar los efectos de los mensajes basura y los programas maliciosos

Ante la preocupación y los costes que supone la lucha contra los mensajes basura y los programas maliciosos, en los últimos años algunos países y regiones han adoptado o reforzado la legislación existente con el fin de proporcionar herramientas para intensificar la lucha contra estos ataques. Los países han establecido leyes y políticas basadas en sus propias necesidades nacionales, como el Reglamento General de Protección de Datos de la Unión Europea (RGPD), que exige el consentimiento del usuario para recopilar sus datos.

Otro ejemplo es el Convenio de la Unión Africana sobre ciberseguridad y protección de datos personales (Convenio de Malabo), que establece un conjunto de normas que los Estados Parte de la región africana deben incorporar a su legislación nacional. En su Artículo 4.3, el Convenio establece que "los Estados Parte prohíben la comercialización directa mediante cualquier tipo de comunicación indirecta que utilice, de una forma u otra, los datos de una persona que no haya dado su consentimiento previo para recibir publicidad directa a través de tales medios". No obstante, el Convenio autoriza la difusión de publicidad directa en determinadas condiciones; por ejemplo, "la comercialización directa por correo electrónico será admisible cuando: a) los datos del destinatario se hayan obtenido directamente de él; b) el destinatario haya dado su consentimiento para ser contactado por los socios comerciales; c) la publicidad directa se refiera a productos o servicios similares prestados por la misma persona física o jurídica" (§ 4.4).

A medida que se vayan aplicando tanto el RGPD de la Unión Europea como el Convenio de Malabo, podremos evaluar y comprender plenamente su eficacia en la reducción de los mensajes basura y los programas maliciosos.

1.3.3 Contribuciones a la Cuestión 3/2 relacionadas con los trabajos para contrarrestar y mitigar los efectos de los mensajes basura y los programas maliciosos

Durante el periodo de estudios, algunos países y Miembros de Sector de la UIT proporcionaron ejemplos adicionales para combatir los mensajes basura y los programas maliciosos:

- En algunas contribuciones se describe cómo se está recopilando información en tiempo real sobre las amenazas a la ciberseguridad para informar y crear estrategias de ciberseguridad resilientes. En el complejo mundo de las tecnologías de la información,

[14] Grupo de Trabajo contra el abuso en la mensajería, programas maliciosos y móviles (M³AAWG). Why M³AAWG?.
[15] Internet Society. The Internet Society's Anti-Spam Toolkit.
[16] GSMA. GSMA Security.
[17] Spamhaus. Spamhaus ZEN + DBL + RPZ.
[18] APWG. Unifying the global response to cybercrime through data exchange research and public awareness.
[19] Anti-Spyware Coalition. Internet, Marketing y Actualidad.

los datos en tiempo real son esenciales para proteger la información. Conocer la situación y, a su vez, disponer de inteligencia sobre ciberamenazas contribuye a que los países y las organizaciones públicas y privadas puedan identificar las amenazas en cuanto surgen y poder así proteger más eficazmente sus recursos. Por lo tanto, es imperativo crear estrategias de ciberresistencia basadas en información de seguridad para proteger a las organizaciones de ataques selectivos y amenazas persistentes.[20]

- En algunas contribuciones se están catalogando los peligros de la ciberdelincuencia para comprender los diversos efectos de los mensajes basura y los programas maliciosos en los usuarios de Internet (por ejemplo, la suplantación de identidad y el fraude en la lotería) y en las empresas (por ejemplo, el acceso no autorizado a los sistemas y los ataques de denegación de servicio). Así, en 2017 Côte d'Ivoire observó los peligros y delitos relacionados con la ciberdelincuencia, que fueron registrados ulteriormente por la Plataforma de lucha contra el ciberdelito (PLCC), y obtuvo información útil y cualitativa para orientar las actividades destinadas a mejorar la educación de los consumidores y las empresas. Se identificaron patrones de fraude en los servicios de dinero móvil, con 453 casos registrados, cuyas pérdidas ascendieron en total a casi 800 000 USD. El fraude en los servicios de dinero móvil es una estafa muy sofisticada, en la que, tras transferir o recibir fondos desde una cuenta de dinero móvil utilizando una sintaxis USSD (*Unstructured Supplementary Service Data*), la víctima recibe una llamada de los estafadores alegando que hubo un problema con la transferencia; si la víctima se deja engañar, los estafadores consiguen retirar dinero a distancia de la cuenta de la víctima utilizando esa misma sintaxis USSD.[21]
- En algunas contribuciones se describe cómo se crean procesos abiertos y transparentes para determinar y promover las medidas que deben tomar los agentes pertinentes para reducir considerablemente las amenazas que plantean los ataques automatizados y distribuidos (por ejemplo, las redes de bots). Las técnicas tradicionales de mitigación de DDoS, basadas en la reserva de recursos por los proveedores de acceso a la red, ya no son eficaces contra las nuevas redes de bots, que pueden ejercer una enorme presión sobre las redes, utilizando más de un terabit de datos por segundo. Para mitigar los peligros derivados de los ciberataques automatizados y distribuidos es necesaria una constante colaboración entre los sectores público y privado.[22]
- Tomando unas sencillas medidas, las empresas pueden protegerse eficazmente contra el peligro que representan los ataques por programas de extorsión. En un reciente aviso sobre este tipo de ataques, el Centro Nacional de Ciberseguridad (NCSC) del Reino Unido recomienda una serie de técnicas sencillas para paliar los riesgos, tales como:

  - mantener actualizados los dispositivos y las redes (por ejemplo, aplicando de inmediato actualizaciones y parches y realizando análisis periódicos);
  - impedir y detectar movimientos laterales en las redes corporativas;
  - utilizar programas antivirus;
  - hacer copias de seguridad de todos los ficheros.[23]

  La lista completa y detallada de recomendaciones puede consultarse en el sitio web del NCSC.[24]
- En algunas contribuciones se describe cómo se ha creado un marco nacional de ciberseguridad flexible que se adapta a las necesidades cambiantes. Por ejemplo, el Reino Unido ha puesto en marcha el programa de ciberdefensa activa, que se centra en la adopción de medidas técnicas positivas destinadas a mejorar el entorno en línea para todos. Este programa ha dado resultados considerables y cuantificables para las redes

20 Documento 2/167 de la CE 2 del UIT-D de Symantec Corporation (Estados Unidos).
21 Documento 2/174 de la CE 2 del UIT-D de Côte d'Ivoire.
22 Documento SG2RGQ/153 y Anexos de la CE 2 del UIT-D de Estados Unidos.
23 Documento SG2RGQ/155 de la CE 2 del UIT-D del Reino Unido.
24 Centro Nacional de Ciberseguridad (NCSC), Guidance: Mitigating malware and ransomware attacks.

gubernamentales. Se ha aplicado en todas las redes de servicios públicos del Reino Unido con el fin de demostrar sus ventajas prácticas y las posibles medidas de seguimiento.[25] Para continuar con sus esfuerzos en este sentido, el Reino Unido actualizó el programa un año después de su puesta en marcha.[26]

- En algunas contribuciones se explican las medidas adoptadas para concienciar a las comunidades vulnerables (por ejemplo, las personas con discapacidad) de que corren mayor riesgo. Los remitentes de mensajes basura y los piratas informáticos utilizan técnicas cada vez más sofisticadas para determinar si sus posibles víctimas padecen algún tipo de discapacidad. En algunos casos, los secuestradores se valen de la discapacidad de una persona para hacerse pasar por ella desde la cuenta de correo electrónico pirateada.[27]
- En algunas contribuciones se describe la introducción de servicios de denuncia de correos electrónicos con fines de *peska* (*phishing*). Una herramienta eficaz para reducir la ciberdelincuencia y el fraude consiste en recopilar correos electrónicos maliciosos y tomar medidas contra los dominios y otras entidades que los contienen. Por ejemplo, en los primeros cuatro meses de funcionamiento del Servicio de Notificación de Correos Electrónicos Sospechosos, el Centro Nacional de Ciberseguridad (NCSC) del Reino Unido y la Policía de Londres eliminaron más de 16 000 amenazas en línea notificadas por los ciudadanos.[28]

[25] Documento SG2RGQ/55 de la CE 2 del UIT-D del Reino Unido.
[26] Documento SG2RGQ/175 de la CE 2 del UIT-D del Reino Unido.
[27] Documento 2/71 de la CE 2 del UIT-D de la Global Initiative for Inclusive Information and Communication Technologies (G3ict).
[28] Documento SG2RGQ/234 de la CE 2 del UIT-D del Reino Unido.

Capítulo 2 – Mejora de la coyuntura nacional en materia de ciberseguridad: oportunidades de sensibilización y capacitación

Las TIC han experimentado en los últimos años un rápido crecimiento e innovación. Además, desempeñan un papel importante para que los países puedan ampliar sus economías digitales y aumentar la prosperidad social. Por añadidura, la pandemia de COVID-19 ha demostrado que las personas son cada vez más dependientes de las TIC en su día a día. Ante esta realidad, resulta primordial que los países sigan adoptando medidas importantes para mejorar y reforzar su coyuntura nacional en materia de ciberseguridad, a fin de protegerse contra los riesgos y problemas de ciberseguridad.

En este capítulo se examinan los principales ámbitos temáticos para mejorar la coyuntura nacional en materia de ciberseguridad, en particular:

- creación de autoridades nacionales de ciberseguridad pertinentes;
- equipos de intervención en caso de emergencia informática (EIEI)/equipos de intervención en caso de incidente de seguridad informática (EIISI)/equipos de intervención en caso de incidente informático (EIII);
- campañas de sensibilización sobre ciberseguridad;
- marcos de gestión de riesgos de ciberseguridad;
- asociaciones público-privadas;
- otras iniciativas de capacitación.

Durante el periodo de estudio, varias entidades presentaron contribuciones sobre estas cuestiones. En el **Anexo 1** figura un compendio de las actividades pertinentes y en curso en materia de ciberseguridad realizadas por los Estados Miembros, las organizaciones, el sector privado y la sociedad civil a escala nacional, regional e internacional. El **Anexo 2** contiene una lista de las prácticas idóneas y las lecciones extraídas facilitadas por algunas de estas entidades.

2.1 Creación de autoridades nacionales de ciberseguridad pertinentes

A medida que se producen nuevos adelantos e innovaciones en el ámbito de las TIC, también aumentan los riesgos y problemas de ciberseguridad. Los gobiernos deben evaluar y mejorar constantemente su coyuntura y sus estrategias nacionales en materia de ciberseguridad para hacer frente a estos problemas, entre otras cosas mediante la creación de las autoridades nacionales de ciberseguridad pertinentes. Durante el periodo de estudio, los Estados Miembros describieron sus criterios para establecer dichas autoridades. Cada país ha adoptado distintos criterios en función de sus estructuras de gobernanza, normativa, reglamentos y políticas nacionales.

Existen ciertas variaciones entre estas autoridades de ciberseguridad en cuanto a experiencia y objetivos, mas por lo general cumplen las mismas funciones esenciales, entre las que se cuentan

el desarrollo y la coordinación de las políticas reguladoras, el desarrollo e implementación de campañas de sensibilización en materia de ciberseguridad, el suministro de información actualizada a los usuarios (desde grandes organizaciones hasta pequeñas empresas y particulares) y la emisión de comunicados y orientaciones sobre incidentes de ciberseguridad. Dada la extensión del panorama de la ciberseguridad, es fundamental que los gobiernos fomenten la coordinación y colaboración entre las distintas autoridades y entidades y entre los sectores público y privado.

Por ejemplo, en el Reino Unido, el Centro Nacional de Ciberseguridad colabora con otras entidades gubernamentales pertinentes y dirige las iniciativas para reducir cuantitativamente los efectos de los ataques de programas de extorsión.[29] En caso de ataque, se recomienda a las organizaciones que se pongan en contacto con la Agencia Nacional contra la Delincuencia, con una empresa certificada para la intervención en caso de incidentes cibernéticos o con la Asociación para el Intercambio de Información sobre Ciberseguridad. El NCSC dirigió la intervención del Reino Unido ante el ataque del programa de extorsión WannaCry, en colaboración con la Agencia Nacional contra la Delincuencia. Cuando se produce un incidente, el centro publica comunicados y orientaciones destinados a las grandes organizaciones, así como a los usuarios particulares y las pequeñas empresas. La información más reciente se anuncia también a través de la cuenta de Twitter del centro (@NCSC).

Brasil adoptó su Estrategia Nacional de Ciberseguridad (E-Ciber), ratificada por el Presidente del país y publicada en febrero de 2020.[30] Esta estrategia de futuro, que representa la filosofía en materia de ciberseguridad del gobierno federal para el periodo 2020-2023, es el resultado de un proceso exhaustivo y completo en el que han participado numerosos agentes, tanto del gobierno como del sector privado y del mundo académico. Con la ratificación de E-Ciber, Brasil ha colmado la laguna legal que antes existía. En el marco de E-Ciber, Brasil ha definido 10 acciones estratégicas, cada una de las cuales consta de medidas e iniciativas. Algunos ejemplos de estas acciones estratégicas son:

- reforzar la gobernanza en materia de ciberseguridad;
- establecer un modelo centralizado de gobernanza sobre ciberseguridad nacional;
- mejorar el marco jurídico nacional en materia de ciberseguridad;
- ampliar la cooperación internacional de Brasil en el ámbito de la ciberseguridad.

En Benin diversas entidades gubernamentales participan en la gestión nacional de las TIC.[31] La Agencia de Servicios y Sistemas de la Información (ASSI), la antigua Agencia Beninesa de Tecnologías de la Información y la Comunicación (ABETIC), es la entidad nacional encargada de poner en marcha programas y proyectos para el desarrollo de servicios y sistemas seguros de información digital en el país:

- realizar los proyectos estrella de administración inteligente y comercio electrónico;
- preparar, actualizar y poner en marcha planes generales para sistemas nacionales de información de ámbito nacional;
- garantizar la coherencia técnica, financiera y práctica de los servicios y sistemas de información nacionales;
- alojar, controlar y proporcionar un acceso seguro a los datos y la información cruciales del Estado y de los operadores de servicios esenciales.

---

[29] Documento SG2RGQ/155 de la CE 2 del UIT-D del Reino Unido.
[30] Documento SG2RGQ/216 de la CE 2 del UIT-D de Brasil.
[31] Documento 2/152 de la CE 2 del UIT-D de Benin.

En Chad, la Agencia Nacional de Seguridad de la Información y Certificación Electrónica (ANSICE), creada en febrero de 2015, depende directamente del Gabinete del Presidente.[32] La agencia empezó a funcionar en enero de 2018 y tiene amplias atribuciones y competencias, incluso sobre la seguridad de los sistemas y redes de información en todo el país.

El Reino Unido también difundió un estudio monográfico actualizado sobre las medidas adoptadas para aplicar buenas prácticas de seguridad para los dispositivos de Internet de las cosas (IoT) de consumo, en particular mediante:

- la publicación del código de prácticas en materia de seguridad de IoT de los consumidores, que establece 13 principios generales (disponible igualmente en alemán, español, francés, japonés, coreano, mandarín y portugués);
- la realización de una consulta pública sobre la normativa y la legislación propuestas;
- la adopción de la norma ETSI EN 303 645[33], la primera norma de aplicación mundial para la seguridad en la IoT, publicada por el Instituto Europeo de Normas de Telecomunicaciones (ETSI); muchas organizaciones ya basan sus programas de certificación y productos en esta norma y en su predecesora, la ETSI TS 103 645;
- la invitación a formular opiniones sobre las propuestas normativas del Reino Unido para recabar la opinión de los interesados acerca del ámbito de aplicación, las obligaciones, los requisitos de seguridad y el plan de aplicación propuestos;
- la invitación al Departamento de Asuntos Digitales, Cultura, Medios de Comunicación y Deporte y al NCSC, para que elaboren de consuno materiales informativos y seminarios web en línea para los fabricantes de IoT, que se han impartido reiteradamente en distintos husos horarios;
- el mantenimiento de un mapa descriptivo de las normas existentes y las organizaciones que ayudan en la aplicación de buenas prácticas en materia de IoT.[34]

2.2 Equipos de intervención en caso de emergencia informática (EIEI)/equipos de intervención en caso de incidente de seguridad informática (EIISI)/equipos de intervención en caso de incidente informático (EIII)

Las capacidades nacionales de respuesta a incidentes (en forma de EIEI/EIISI/EIII) son instrumentos fundamentales para hacer frente a los problemas de ciberseguridad operativa. Estas capacidades facilitan la coordinación de la información en materia de ciberseguridad y las respuestas a los incidentes de seguridad. Durante el periodo de estudio, la Comisión de Estudio recibió importantes contribuciones de los Estados Miembros y Miembros de Sector de la UIT sobre el tema, muchas de las cuales compartían la opinión de que los EIEI/EIISI/EIII nacionales han de ser el principal punto de contacto para las cuestiones de ciberseguridad y actuar de coordinadores de las respuestas a los incidentes.

Por ejemplo, el equipo de intervención en caso de incidente informático de Bhután (BtCIRT) se creó en abril de 2016 para mejorar la ciberseguridad en el país, facilitar la coordinación de la información sobre ciberseguridad y establecer capacidades nacionales para la gestión de incidentes de seguridad informática.[35] El BtCIRT depende del Departamento de Tecnologías de la Información y Telecomunicaciones del Ministerio de Información y Comunicaciones. En virtud de su mandato, el BtCIRT actúa como punto de contacto nacional para cuestiones de

[32] Documento 2/136 de la CE 2 del UIT-D de Chad.
[33] ETSI. Norma ETSI EN 303 645, Cyber Security for Consumer Internet of Things: Baseline Requirements.
[34] Documento SG2RGQ/241 de la CE 2 del UIT-D del Reino Unido.
[35] Documento SG2RGQ/79 de la CE 2 del UIT-D de Bhután.

ciberseguridad y representa al país en los foros internacionales. Disponer de una organización que coordine todas las iniciativas de ciberseguridad garantiza que no se dupliquen los esfuerzos ni las actuaciones. Como la mayoría de los foros y grupos internacionales centrados en la ciberseguridad se comunican con los EIII cuyo mandato es de alcance nacional, es importante que los gobiernos designen a un EIII o una única organización para gestionar las iniciativas y planes nacionales de ciberseguridad.

Si bien el BtCIRT fue designado punto de contacto para cuestiones relacionadas con la ciberseguridad en Bhután, ganarse la confianza de las partes interesadas ha supuesto todo un reto para el equipo, debido principalmente a sus limitadas capacidades técnicas y a que es un equipo relativamente nuevo. Además, las grandes empresas, como los operadores de telecomunicaciones y los bancos, ya cuentan con una sólida infraestructura de TIC con capacidades técnicas, lo que dificulta la cooperación entre el gobierno y estas grandes corporaciones. La colaboración y cooperación entre las partes interesadas, especialmente los proveedores de servicios de Internet y los EIII, resulta esencial para poder ofrecer soluciones de seguridad concertadas a los usuarios de Internet. Bhután recurrió a organizaciones internacionales para que le ayudaran a crear la capacidad técnica fundamental del BtCIRT.

Por último, la empresa lituana NRD Cyber Security propuso que, además de servir como principal punto de contacto para los incidentes de ciberseguridad y ocuparse de coordinar las respuestas, los EIISI nacionales y sectoriales también deberían actuar de facilitadores o catalizadores para crear capacidades independientes y distribuidas más resilientes contra las ciberamenazas en el país.[36]

2.3 Campañas de sensibilización

Si bien son muy diversas las partes interesadas –desde gobiernos y entidades comerciales hasta organizaciones comunitarias y ciudadanos individuales– que utilizan intensamente las TIC en todo el mundo, muchos usuarios no son plenamente conscientes de los riesgos de ciberseguridad inherentes a dicha utilización. Para ciertos países en desarrollo, la mayor dificultad radica en la falta de sensibilización de los usuarios. En las contribuciones recibidas durante el periodo de estudio, existe un convencimiento generalizado de que las campañas de sensibilización en materia de ciberseguridad desempeñan un papel importante a la hora de superar esas dificultades. El objetivo principal de estas campañas es fomentar la adopción de un comportamiento seguro en línea.

Los países y las empresas están buscando formas creativas de lanzar campañas eficaces, incluyendo la forma de llegar a un amplio conjunto de usuarios.

Por ejemplo, México informó de su experiencia en el desarrollo y realización de una encuesta a los usuarios de Internet, que puede servir de orientación a la hora de concebir campañas de sensibilización sobre ciberseguridad.[37]

Algunos países han utilizado las encuestas para identificar las principales preocupaciones de los ciudadanos y desarrollar campañas de sensibilización a medida basadas en los resultados. México ha extraído de su experiencia las siguientes lecciones:

– instalar y actualizar la protección antivirus;

[36] Documento 2/172 de la CE 2 del UIT-D de NRD Cyber Security (CS) (Lituania).
[37] Documento 2/165 de la CE 2 del UIT-D de México.

- cambiar regularmente las contraseñas y asegurarse de que son fuertes (es decir, que utilizan una combinación de números, letras y caracteres especiales);
- hacer copias de seguridad de los datos con regularidad;
- conectarse únicamente a redes públicas seguras.

Otro ejemplo es el del BtCIRT de Bhután, que creó programas de sensibilización adaptados a las necesidades de ciberseguridad derivadas de la actividad profesional y personal de los usuarios finales de todo el país.[38] A los participantes se les enseñó cómo se ejecutan los ataques a través de la ingeniería social y las estafas de *peska* (*phishing*), cómo comunicarse de forma segura utilizando el correo electrónico y los servicios de las redes sociales y cuáles son las amenazas más comunes y las respuestas para remediarlas. Los programas de sensibilización de Bhután han resultado muy eficaces para sensibilizar a los usuarios sobre los riesgos de seguridad y han recibido comentarios positivos. Aunque actualmente se centran en los funcionarios públicos, el equipo de BtCIRT quiere ampliar sus esfuerzos a los niños y otros usuarios vulnerables.

Otro ejemplo creativo proporcionado por Bhután es el lanzamiento de un concurso anual de sitios web nacionales, organizado por el Departamento de Tecnología de la Información y Telecomunicaciones del Ministerio de Información y Comunicaciones.[39] Todos los sitios web gubernamentales se presentan al concurso, en el que se selecciona el mejor sitio web del país en función de los siguientes criterios básicos:

- facilidad de uso y fiabilidad;
- contenido y vigencia;
- seguridad y disponibilidad;
- apariencia;
- diseño interactivo.

Asimismo, en noviembre de 2019, Brasil lanzó la campaña de sensibilización sobre ciberseguridad #ConexãoSegura (Conexión Segura) a través de la Agencia Nacional de Telecomunicaciones de Brasil (Anatel).[40] La campaña ofrecía consejos a los consumidores sobre la protección de los datos personales y la creación de contraseñas seguras. La campaña surgió a raíz de las quejas manifestadas por los consumidores sobre intentos de estafa y de las dudas sobre cómo salvaguardar los datos personales. Ante la irrupción de la pandemia de COVID-19 y el aumento de nuevas estafas, se crearon nuevos artículos sobre el fraude y las estafas de la COVID-19 para ayudar a los usuarios. Los artículos también se difundieron por las redes sociales de Anatel, como Facebook, Twitter, Instagram y LinkedIn. Algunas de las principales prácticas idóneas de la campaña fueron:

- utilizar todas las opciones de seguridad que ofrecen las aplicaciones móviles, como la autenticación de dos factores;
- crear contraseñas fuertes y seguras, que consten de letras mayúsculas y minúsculas, números y caracteres especiales;
- desconfiar de los correos electrónicos y mensajes con facturas adjuntas y ponerse siempre en contacto con el servicio de atención al cliente de la empresa para verificar la autenticidad de las mismas;

[38] Documento SG2RGQ/79 de la CE 2 del UIT-D de Bhután.
[39] Documento SG2RGQ/135 de la CE 2 del UIT-D de Bhután.
[40] Documento SG2RGQ/215 de la CE 2 del UIT-D de Brasil.

- no proporcionar información personal ni contraseñas al responder a llamadas desconocidas.[41]

El Reino Unido presentó un estudio monográfico sobre las prácticas idóneas de resiliencia en materia de ciberseguridad para las pequeñas y medianas empresas, en el que se exponen las iniciativas que se están adoptando para mejorar la resiliencia cibernética de las organizaciones de todo el país.[42] Un ejemplo de tales iniciativas es la campaña de comunicación Cyber Aware, que, más allá de la simple sensibilización, pretende fomentar la adopción generalizada de comportamientos básicos de ciberseguridad. La campaña, dirigida al público y a las pequeñas empresas, se puso en marcha en abril de 2020, tras haber sido reformulada rápidamente para hacer frente al nuevo paradigma de ciberamenazas generado por la pandemia de COVID-19. La campaña promovía medidas de mitigación aplicables, complementadas por nuevas orientaciones sobre cómo trabajar desde casa de forma segura, reconvertir la empresa en un negocio en línea y utilizar las videoconferencias. Otras herramientas son:

- Guía para pequeñas empresas: ciberseguridad;
- Guía para pequeñas empresas: respuesta y recuperación, que describe un plan continuo para ayudar a las pymes a prepararse para incidentes cibernéticos y mitigar sus posibles efectos;
- Exercise in a Box, una herramienta gratuita en línea que ayuda a las pymes a comprobar su resiliencia cibernética y seguir microcursos sin precisar de grandes conocimientos técnicos;
- Guía sobre la COVID-19 para ayudar a las empresas a mantenerse seguras y, a su vez, adaptarse a la pandemia, que incluye temas como el teletrabajo y reconvertir las operaciones comerciales en un modelo en línea.

El Reino Unido también presentó en detalle su plan de certificación respaldado por el gobierno, Cyber Essentials, destinado a proteger a las empresas contra los ciberataques más comunes sin exigirles que se ajusten a múltiples y complejas normas. Cyber Essentials se ha diseñado para que resulte útil a todas las organizaciones, incluso a las que no disponen de conocimientos previos de ciberseguridad ni de un equipo especializado en ese tema.

2.4 Marcos sobre riesgos de ciberseguridad

Los marcos relativos a riesgos de ciberseguridad son fundamentales para las organizaciones gubernamentales y no gubernamentales. Suelen ser marcos de carácter voluntario que proporcionan directrices y prácticas idóneas para la gestión de los riesgos digitales. Durante el periodo de estudio, la Comisión de Estudio recibió contribuciones en las que se describen diferentes ejemplos y planteamientos de marcos relativos a riesgos de ciberseguridad.

Por ejemplo, el Instituto Nacional de Normas y Tecnología (NIST) de Estados Unidos ha actualizado recientemente su marco para mejorar la ciberseguridad de las infraestructuras esenciales.[43] Se trata de un marco proactivo orientado a las empresas para la gestión voluntaria del ciberriesgo, diseñado para empresas de todos los tamaños pertenecientes a diversos sectores económicos. Ofrece un punto de partida y un lenguaje comunes para evaluar el ciberriesgo, y es fácilmente adaptable, lo que permite a las organizaciones –con independencia

41 Para más información sobre la campaña "Conexión segura" de Anatel, consulte el siguiente sitio web https://www.anatel.gov.br/consumidor/component/content/article/109-manchetes/960-conexaoseguro-confira-dicas-para-proteger-dados-pessoais.
42 Documento SG2RGQ/272 de la CE 2 del UIT-D del Reino Unido.
43 Documento SG2RGQ/151 de la CE 2 del UIT-D de Estados Unidos.

de su tamaño, grado de riesgo de ciberseguridad o sofisticación de la ciberseguridad– aplicar los principios y las prácticas idóneas de gestión de riesgos para mejorar la seguridad y la resiliencia de las infraestructuras esenciales.

El marco se desarrolló gracias a la exitosa colaboración público-privada en la gestión de riesgos de ciberseguridad, tras un proceso de desarrollo voluntario de un año de duración que incluyó las aportaciones de más de 3 000 partes interesadas de los sectores industriales, el mundo académico, el gobierno y los socios internacionales.

El marco se basa en normas internacionales existentes, directrices y prácticas idóneas del sector que han demostrado su eficacia para proteger los sistemas informáticos contra las ciberamenazas, garantizar la confidencialidad de las empresas y salvaguardar la privacidad individual y las libertades civiles, con objeto de fomentar la protección de las infraestructuras esenciales mediante la gestión de riesgos. Asimismo, el marco proporciona una estructura para organizar las prácticas, así como herramientas para facilitar la utilización y adopción de normas y prácticas. Dado que hace referencia a normas de ciberseguridad reconocidas a nivel mundial, el marco también tiene la flexibilidad de servir como modelo internacional para la gestión de ciberriesgos.

Basándose en los comentarios de las partes interesadas, el NIST realizó las siguientes actualizaciones en la versión 1.1 del marco:

- declaración de la aplicabilidad del marco a la "tecnología", que comprende, como mínimo, la tecnología de la información, la tecnología operativa, los sistemas ciberfísicos y la IoT;
- mejora de las orientaciones para aplicar el marco a la gestión de riesgos de la cadena de suministro;
- síntesis de la pertinencia y la utilidad de las mediciones previstas en el marco para que las organizaciones puedan autoevaluarse;
- mayor información sobre la autoevaluación del riesgo de ciberseguridad;
- una mayor consideración de los requisitos de autorización, autenticación, protección de la identidad y divulgación de la vulnerabilidad;
- actualización administrativa de las referencias informativas para incorporar los avances en las normas y directrices de las organizaciones públicas y privadas.

Además, en Bhután, la Real Autoridad Monetaria (el banco central) ha promulgado una directiva para fomentar la aplicación de un marco de ciberseguridad a las instituciones financieras con el fin de mejorar la resiliencia del sistema bancario ante ciberriesgos desconocidos y avanzados.[44] La directiva abarca los siguientes ámbitos:

- Todos los bancos miembros deben procurar el cumplimiento de la norma de seguridad de datos relativa al sector de las tarjetas de pago, destinada a proteger los datos de los titulares de las tarjetas. Además, los bancos deben aplicar la norma ISO/IEC 27001:2013, relativa a los sistemas de gestión de la seguridad de la información, para complementar sus propias medidas de ciberseguridad.
- La directiva subraya la necesidad de crear un equipo de respuesta cibernética en las instituciones financieras para promover la colaboración activa y el intercambio eficaz de información sobre ciberseguridad entre los bancos y la Real Autoridad Monetaria. El equipo se encargaría de vigilar activamente las ciberamenazas, planificar y coordinar las medidas para prevenir los riesgos de ciberseguridad e informar sin dilación de cualquier incidente al supervisor o a las autoridades pertinentes. Recientemente se ha constituido

[44] Documento SG2RGQ/135 de la CE 2 del UIT-D de Bhután.

un equipo cibernético para los bancos, cuya función rectora ha sido asumida por la Real Autoridad Monetaria.
- Los bancos miembros también deben aplicar el marco de control de ciberseguridad correspondiente y las acciones de respuesta como medida inmediata para garantizar la seguridad básica de la información.

Por su parte, China ha creado un índice de evaluación para medir la visión nacional en la planificación, el desarrollo y la aplicación de la seguridad de las redes, utilizando tres niveles de indicadores cada vez más complejos.[45] En el primer nivel se evalúan cinco indicadores:

- *Política*: estrategias nacionales, legislación, organismos gubernamentales y cooperación internacional.
- *Industria*: desarrollo de la industria de seguridad de las redes en un entorno comercial, incluido el entorno de desarrollo, la escala, la competitividad de las empresas, la sostenibilidad, etc.
- *Tecnología*: investigación y desarrollo y nivel de aplicación de la seguridad nacional en el ámbito de la tecnología, incluidos los proyectos específicos de investigación científica, la inversión, las normas técnicas y la formación del personal.
- *Capacidad*: nivel de protección de seguridad de la red y prevención de amenazas, incluida la percepción del riesgo, la protección de la seguridad, la respuesta en caso de emergencia y la defensa activa.
- *Recursos*: recursos necesarios para apoyar la capacitación, incluidos los recursos de infraestructura de red, la sensibilización respecto de la seguridad, la influencia internacional, etc.

El índice comprende además 19 indicadores de segundo nivel y 53 de tercer nivel. Según el sistema de puntuación del índice, cada indicador vale entre 0 y 1 punto, siendo 53 la máxima puntuación posible. Los cálculos de cada indicador se basan en información pública oficial divulgada en sitios web nacionales e internacionales y por instituciones de investigación.

2.5 Asociaciones público-privadas

Las entidades gubernamentales no pueden mejorar por sí mismas la coyuntura nacional en materia de ciberseguridad. El éxito de las iniciativas y los proyectos de ciberseguridad exige una sólida colaboración entre entidades del sector público y privado.

En Estados Unidos, el Instituto Nacional de Normas y Tecnología desarrolló su marco para mejorar la ciberseguridad de la infraestructura esencial a través de un proceso de cooperación resultante de una asociación público-privada.[46] Como se expone con más detalle en la sección 2.4, el instituto se aseguró de que todas las partes interesadas participaran en el desarrollo de la actualización para fomentar la máxima observancia del marco. Al hacer partícipes a los distintos interesados e incorporar sus comentarios a la versión 1.1 del marco, es más probable que estos se adhieran y apliquen las prácticas idóneas, directrices y normas que incorpora.

En la República de Corea, el Ministerio de Ciencia y TIC elaboró el Plan Básico de Ciberseguridad Nacional de 2019 para el sector privado en consulta con las partes interesadas pertinentes, en particular, el mundo académico, la industria y las organizaciones públicas.[47] El plan establece dos objetivos: garantizar un ciberespacio seguro y desarrollar la industria de la seguridad de la información. A tal efecto, los principales proyectos estratégicos tenían por objeto ampliar

[45] Documento 2/155 de la CE 2 del UIT-D de China.
[46] Documento SG2RGQ/151 de la CE 2 del UIT-D de Estados Unidos.
[47] Documento 2/168 de la CE 2 del UIT-D de la República de Corea.

la red de ciberseguridad, promover la industria de la seguridad de la información y reforzar la infraestructura de seguridad de la información.

Habida cuenta de la rápida evolución del entorno de las TIC, el ministerio tiene previsto actualizar el plan cada año. El Consejo de consulta público-privada de la República de Corea también se reúne dos veces al año para supervisar los progresos del plan e identificar los aspectos susceptibles de mejora.

La estrategia nacional de ciberseguridad de Brasil, E-Ciber, descrita en la sección 2.1, es otro ejemplo de la importancia de las asociaciones público-privadas (PPP) en el desarrollo de estrategias nacionales de ciberseguridad. Las PPP figuran entre las acciones estratégicas fundamentales contenidas en E-Ciber, que comprende la promoción de un entorno colaborativo, participativo, seguro y fiable entre los sectores público y privado y la sociedad civil, y la ampliación de las asociaciones de ciberseguridad entre los sectores público y privado, el mundo académico y la sociedad civil.

Brasil, en otro buen ejemplo de colaboración entre el sector público y el privado, expuso su experiencia en la realización en 2018 de un cibersimulacro nacional, denominado Ejercicio Ciber Guardián, focalizado en las infraestructuras esenciales nacionales.[48] En 2019, Brasil llevó a cabo un ejercicio de seguimiento, ampliando considerablemente la gama de participantes para incluir a representantes de los Ministerios de Defensa, Justicia y Asuntos Exteriores, la Oficina de Seguridad Institucional, las fuerzas militares, los organismos del gobierno federal como Anatel, los EIISI nacionales, el Banco Central de Brasil, los bancos públicos y privados, las empresas nucleares, eléctricas y de telecomunicaciones, los investigadores académicos y los observadores regionales e internacionales invitados.

Otros ejemplos de PPP son los EIEI/EIISI/EIII. A través de estos equipos, los organismos públicos y el sector privado pueden cooperar para resolver incidentes de ciberseguridad. No obstante, la colaboración y la confianza son necesarias para garantizar la eficacia de estos equipos.

2.6 Otras medidas/iniciativas de creación de capacidad

2.6.1 Establecimiento de instituciones de educación en ciberseguridad

Ante la evidente la necesidad de invertir en formación y educación en ciberseguridad para hacer frente a los crecientes desafíos que esta última conlleva, muchos gobiernos han creado instituciones educativas encargadas de formar a la próxima generación de expertos en ciberseguridad. Durante el periodo de estudios, diversos Estados Miembros de la UIT han presentado contribuciones en las que se reconoce la necesidad de tomar medidas en ese sentido, entre ellas medidas encaminadas a afianzar las relaciones entre los actores públicos, las universidades y los centros de investigación.

Por ejemplo, en 2015, Chad creó la Escuela Nacional Superior de Tecnologías de la Información y la Comunicación (ENASTIC), lo que, sin lugar a dudas, puso de manifiesto la voluntad política de las más altas esferas del país de instaurar un marco de educación avanzada en TIC (incluidas titulaciones en ciberseguridad, redes, telecomunicaciones, etc.).[49]

[48] Documento SG2RGQ/214 de la CE 2 del UIT-D de Brasil.
[49] Documento 2/136 de la CE 2 del UIT-D de Chad.

Del mismo modo, Senegal creó la Escuela Nacional de Ciberseguridad (ENC), que aplica un enfoque regional a efectos de la creación de capacidad y la concienciación de los responsables de la toma de decisiones, los altos cargos del sector de la defensa y otras partes implicadas en el ecosistema digital de la región.[50]

Entre las funciones principales de dicha escuela figuran las siguientes:

- formar y sensibilizar a los funcionarios estatales, los trabajadores y los estudiantes senegaleses y extranjeros, así como a los miembros de los sectores público y privado, en cuestiones relacionadas con la ciberseguridad, para mejorar su comprensión de las amenazas y los riesgos conexos;
- formar regularmente a los miembros del personal de los EIEI/EIISI, de tal manera que puedan hacer frente a los ciberataques más sofisticados;
- formar periódicamente a los miembros del personal de las instituciones estatales y subregionales, con objeto de que adquieran la capacidad y los conocimientos necesarios para prepararse, protegerse, intervenir y recuperarse en caso de incidente.

2.6.2 Otras iniciativas de creación de capacidad

A lo largo del periodo de estudios, el Coordinador de Ciberseguridad de la Oficina de Desarrollo de las Telecomunicaciones (BDT) rindió cuenta periódicamente de la evolución del programa de trabajo de la BDT, incluidas sus diversas iniciativas en materia de creación de capacidad. La Oficina ha colaborado con diferentes organizaciones y entidades en la provisión de cursos de capacitación para países en desarrollo, en cuyo marco se realizaron cibersimulacros, se prestó asistencia con miras al desarrollo de EIISI y se celebraron sesiones de formación. Estas iniciativas también han ocupado un lugar destacado en las contribuciones de los Estados Miembros y los Miembros de Sector. Para obtener más información al respecto, véase el **Anexo 1**.

[50] Documento SG2RGQ/146 de la CE 2 del UIT-D de Senegal.

Capítulo 3 – Protección de la infancia en línea

3.1 Consideraciones generales

Hoy en día, Internet ya no es ese banco de conocimientos –esa "enorme y desordenada biblioteca"– que conocimos en la era de la Web 1.0. Ahora se ha convertido en una plataforma de comunicación para todo tipo de usuarios, niños incluidos. De hecho, según el Fondo de las Naciones Unidas para la Infancia (UNICEF), un tercio de los usuarios de Internet de todo el mundo son niños.[51]

El tipo de las amenazas a las que se enfrentan los niños en línea ha cambiado. Si las amenazas anteriores revestían un carácter puramente informativo –por ejemplo, el acceso a información sobre drogas, pornografía o movimientos extremistas–, las amenazas actuales también son de naturaleza conductual, véanse en especial la falta de socialización, la adicción al juego, el gasto incontrolado, el ciberacoso, la divulgación de datos personales y las relaciones con personas peligrosas.

En el último decenio, la comunidad tecnológica no ha cesado de inventar formas de proteger a los niños de los sitios que contienen información inapropiada; no obstante, desarrolladores y padres se enfrentan ahora a un nuevo desafío: cómo integrar adecuadamente a los usuarios jóvenes en el espacio digital y cómo controlar y corregir rápidamente ciertas conductas virtuales. Con el rápido desarrollo de la tecnología de Internet, la cuestión de la protección de la infancia, sobre la que existe un consenso mundial, se ha extendido de forma natural al ciberespacio. La seguridad del ciberespacio es primordial para que los niños puedan empezar a utilizar dispositivos digitales y a navegar por Internet.

En la Declaración de Buenos Aires, adoptada por la CMDT-17, se estipula "que las oportunidades que ofrecen las telecomunicaciones/TIC deberían explotarse a fondo con el fin de conseguir un acceso equitativo a las telecomunicaciones/TIC y a las innovaciones que fomentan el desarrollo socioeconómico sostenible, la mitigación de la pobreza, la creación de empleo, la igualdad de género, la protección de la infancia en línea, la iniciativa empresarial y la promoción de la inclusión digital y el empoderamiento universal".[52]

En la Resolución 179 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios de la UIT y la Resolución 67 (Rev. Buenos Aires, 2017) de la CMDT se establece el papel que deben desempeñar la UIT y el UIT-D en la protección de la infancia en línea.

Como ha demostrado la pandemia de COVID-19, las pautas conductuales de los atacantes y las redes delictivas se hallan en constante evolución y, ahora, los delincuentes se aprovechan del hecho de que muchos niños están pasando bastante más tiempo en línea de lo habitual. Estas circunstancias hicieron oportuna la publicación de las Directrices de 2020 sobre la Protección

[51] UNICEF. "El Estado Mundial de la Infancia 2017", diciembre de 2017.
[52] UIT. Conferencia Mundial de Desarrollo de las Telecomunicaciones (Buenos Aires, 2017), Declaración de Buenos Aires, octubre de 2017.

de la Infancia en Línea, cuyo objetivo es salvaguardar el bienestar, la integridad y la seguridad de los niños.[53]

Estas directrices fueron redactadas conjuntamente por la UIT y un grupo de trabajo de autores colaboradores de grandes instituciones activas en el sector de las TIC, así como en ámbitos relacionados con los derechos y la protección de la infancia (en línea), y constituyen un conjunto exhaustivo de recomendaciones para todas las partes interesadas sobre cómo contribuir al desarrollo de un entorno en línea seguro y habilitador para niños y jóvenes. El objetivo de las directrices es crear conciencia sobre el alcance de la protección de la infancia en línea y proporcionar recursos y herramientas que ayuden a los niños y a sus familias a desarrollar competencias digitales, así como apoyar a las partes interesadas del sector y del gobierno en la elaboración de políticas y estrategias corporativas y nacionales de protección de la infancia en línea. Las directrices van dirigidas a niños, padres, educadores, empresas y responsables políticos, y han sido concebidas como una hoja de ruta que puede adaptarse a las costumbres y las leyes nacionales y locales.

En virtud del plan estratégico de la UIT descrito en la Resolución 71 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios de la UIT, uno de los objetivos del UIT-D es "fomentar el desarrollo y la utilización de las telecomunicaciones/TIC y aplicaciones a fin de empoderar a las personas y a las sociedades para el desarrollo sostenible" (§ D.4). En concreto, el UIT-D ha de proporcionar "productos y servicios relativos a la inclusión digital de las niñas y las mujeres y de las personas con necesidades específicas (ancianos, jóvenes, niños y pueblos indígenas, entre otros), como la información sobre estrategias, políticas y prácticas de inclusión digital, desarrollo de capacidades digitales, herramientas y directrices y foros de debate para la compartición de prácticas y estrategias", con objetivos tales como el fomento de la protección de la infancia en línea (§ D.4-3).

Las actividades llevadas a cabo por el UIT-D y sus miembros a efectos de la protección de la infancia se abordan en el apartado 2 d) del mandato de la Cuestión 3/2:

d) continuar recabando experiencias nacionales de los Estados Miembros en ciberseguridad y protección de la infancia en línea e identificar y analizar los temas en común entre estas experiencias, utilizando esa información para proporcionar los insumos necesarios con miras a la elaboración de directrices que brinden asistencia a los Estados Miembros en el desarrollo de mecanismos eficaces para garantizar la seguridad en el entorno digital.

3.2 Mejores prácticas y tendencias comunes entre los Estados Miembros de la UIT

Durante el ciclo de estudios, las principales actividades de protección de la infancia en línea de los Estados Miembros giraron en torno a la sensibilización, la normalización y la realización de encuestas temáticas.

Sensibilización

La protección de la infancia en el ciberespacio es un tema heterogéneo, para el que se requieren no solo herramientas y plataformas, sino también datos adecuados. Los programas culturales deberían contribuir a la difusión de estos recursos a la sociedad en su conjunto.

[53] UIT. Directrices sobre Protección de la Infancia en Línea.

Por ejemplo, la Organización de Tecnologías de la Información del Irán desarrolló el proyecto KOVA, dedicado a los niños e Internet y encaminado a su protección en el ciberespacio, el cual figuró entre los galardonados en el Concurso de Premios de la Cumbre Mundial sobre la Sociedad de la Información de 2018.

En 2016, habida cuenta del vertiginoso desarrollo de la infraestructura de Internet en los años precedentes y del gran número de usuarios jóvenes de Internet, niños incluidos, el gobierno iraní puso en marcha un programa nacional en favor de la protección de la infancia en la red. En el marco de este programa, el Ministerio de TIC presentó el proyecto KOVA, con el objetivo de sensibilizar a niños y padres sobre los peligros de Internet y darles a conocer los medios disponibles para proteger a la infancia en línea. Los principales objetivos del proyecto son:

- detectar las amenazas más graves para los niños en el ciberespacio y ofrecer soluciones y servicios de protección jurídica;
- sensibilizar a los alumnos de primaria y secundaria, a los docentes y a los padres acerca de las distintas amenazas que se ciernen sobre los niños en función de su edad;
- ayudar a niños y adolescentes a utilizar las redes sociales e Internet de forma segura; y
- responder a las preguntas planteadas por niños, adolescentes, docentes y padres sobre los desafíos inherentes a la seguridad en el ciberespacio.

A fin de lograr los objetivos de este proyecto, se utilizó una amplia gama de herramientas y métodos (como obras de teatro, películas y animaciones) para instruir a los niños sobre la seguridad en línea. En la primera fase del proyecto, más de 200 000 alumnos de 900 escuelas recibieron formación. El objetivo de la segunda fase es llegar a 4 000 escuelas.[54]

En Bhután, el número de usuarios de Internet ha aumentado en más del 28 por ciento desde 2016, puesto que el acceso es cada vez más sencillo, la conexión es cada vez más asequible y los teléfonos inteligentes son cada vez más baratos. El hecho de que la mayoría de los escolares tenga acceso a un teléfono inteligente conlleva un mayor riesgo de que se produzcan incidentes de seguridad. Bhután sigue careciendo de un plan de estudios en materia de ciberseguridad, dado que el creciente uso de Internet y de los dispositivos móviles es una tendencia moderna. No obstante, es crucial que los gobiernos se adapten a los nuevos tiempos e incluyan la ciberseguridad en sus planes de estudio. Algunas facultades privadas de Bhután han empezado a plantearse cómo ofrecer programas de grado conexos, especialmente en ciberseguridad. Los escolares deben ser conscientes de estos riesgos, ya que son más vulnerables a los ataques de suplantación de identidad (*phishing*) y al juego en línea.[55]

En respuesta a estas consideraciones, tras haber examinado los hábitos y comportamientos en línea de los niños, Bhután está elaborando vídeos de animación sobre temas como la trata de niños, el ciberacoso, la privacidad y la seguridad de los juegos en línea, que se emitirán en la televisión nacional. También se están elaborando carteles y folletos que presentan las prácticas idóneas en materia de ciberseguridad, dirigidos a los estudiantes, y que se distribuirán en varias escuelas del país. Bhután está también creando un grupo de trabajo de ámbito nacional en el que estarán representados diversos organismos para elaborar las directrices de protección de la infancia en línea en el país.[56]

---

[54] Documento 2/82 de la CE 2 del UIT-D de la Universidad de Ciencia y Tecnología de Irán (República Islámica del Irán).
[55] Documento SG2RGQ/79 de la CE 2 del UIT-D de Bhután.
[56] Documento 2/385 de la CE 2 del UIT-D de Bhután.

Cada año, China celebra una semana nacional de divulgación de la seguridad en la red, con el objetivo de difundir información sobre este tema y mejorar las capacidades de protección en línea de la población en su conjunto, a través de exposiciones, foros, concursos, conferencias, jornadas publicitarias temáticas y otras actividades. En este marco se imparten conferencias sobre seguridad en la red, con miras al intercambio de conocimientos y competencias acordes a las necesidades de los diferentes grupos, entre ellos estudiantes de primaria y secundaria, personas de edad avanzada y grupos especiales (por ejemplo, personas con discapacidad), en función de su nivel de conocimiento de las tecnologías de la información.[57]

Estados Unidos ofrece a padres y docentes información sobre prácticas idóneas para niños y adolescentes con campañas como: What you post can last a lifetime! (lo que publicas puede durar toda la vida), Be aware of what is being shared! (cuidado con lo que compartes), Be careful about too much personal information! (no te pases con la información personal), Post only about others what you would like them to post about you! (publica de los demás lo que querrías que publicasen de ti), Own your online presence by limiting who can see and share information! (controla tu presencia en línea limitando quién puede ver y compartir la información), y Know what data are being collected!(sé consciente de los datos que se obtienen de ti).[58]

Normativa

Dada la amplia disponibilidad de tecnologías de la información, los gobiernos están tomando serias medidas reglamentarias para garantizar la seguridad de todos los ciudadanos dotados de acceso a Internet, en particular los menores. Aunque la legislación en materia de ciberseguridad difiere ligeramente de un país a otro, las raíces del problema son comunes.

Uno de los principales motivos de la promulgación de estas normativas es que los niños en edad de cursar enseñanza preescolar y primaria son especialmente vulnerables en Internet y pueden sufrir con facilidad actos de hostigamiento de depredadores en línea (personas que acosan sexualmente a menores en la red), humillación, captación en Internet con fines sexuales (por desconocidos que se ganan su confianza para sus propios fines) y utilización indebida de sus datos personales.

Los niños se han convertido paulatinamente en el grupo de mayor riesgo en lo que a divulgación de información privada y robo de identidad se refiere. Por tanto, la protección de los datos personales de los niños es una cuestión sumamente acuciante.

Por ejemplo, China ha promulgado un reglamento especial sobre ciberprotección de la información personal infantil, por el que se regula el ciclo completo de recogida, almacenamiento, uso, transferencia y divulgación de datos personales de menores.[59] Este reglamento prevé protecciones especiales, principios claros y un sistema de gobernanza cooperativa, con el objetivo de crear un entorno en línea beneficioso para el crecimiento saludable de los niños. Entre dichas protecciones especiales figuran los derechos de supresión y no divulgación de los datos personales de los niños, mientras que los principios se centran en la necesidad legítima, el consentimiento informado, el propósito claro, la seguridad y el uso legal. El reglamento se aplica principalmente a la protección de la información personal de los niños menores de 14 años.

---

57 Documento 2/286 de la CE 2 del UIT-D de China.
58 Documento 2/400 de la CE 2 del UIT-D de Estados Unidos.
59 Documento SG2RGQ/179 de la CE 2 del UIT-D de China.

En diciembre de 2010, la Federación de Rusia promulgó una ley sobre protección de la infancia contra la información nociva para su salud y su desarrollo, que garantiza la seguridad de la información de los menores y establece los procedimientos y condiciones aplicables a la difusión de información entre niños.[60]

Además, la Ley de Medios de Comunicación de la Federación de Rusia prohíbe la difusión en los medios de comunicación o en cualquier red de información y comunicación (entre ellas Internet) de información sobre menores que hayan sido víctimas de actos (u omisiones) de carácter ilícito, incluidos:

- el apellido, el nombre o el patronímico;
- imágenes fotográficas o de vídeo del menor o de sus padres u otros representantes legales;
- la fecha de nacimiento del menor;
- grabaciones de audio de la voz del menor;
- el lugar de residencia o el domicilio temporal del menor;
- el lugar donde el menor estudia o trabaja; y
- cualquier otro dato que pueda utilizarse para identificar al menor directa o indirectamente.[61]

Encuestas temáticas

La UIT ha prestado asistencia técnica en el actual proceso de redacción de la estrategia nacional de ciberseguridad de Bhután.[62] En ese contexto, se llevó a cabo una encuesta a 126 estudiantes (de una media de 16 años), que incluyó una serie de preguntas de respuesta múltiple con el objetivo de evaluar el uso de Internet, los incidentes de seguridad (entre ellos el ciberacoso) y la prevalencia de virus informáticos o delitos cometidos por estudiantes.

La encuesta reveló que los estudiantes utilizaban Internet profusamente. Casi todos los estudiantes que participaron en la encuesta utilizaban Internet, y más del 40 por ciento dedicaba a ello más de dos horas al día. La ciberseguridad constituía un tema acuciante para los estudiantes: si bien casi el 40 por ciento indicó haber sufrido una infección por un programa malicioso, solo alrededor del 10 por ciento afirmó utilizar programas antivirus.

En cuanto a la educación en materia de ciberseguridad, la escuela sigue siendo una importante fuente de conocimiento para los estudiantes. Casi el 40 por ciento de los estudiantes declaró haber aprendido sobre ciberseguridad en la escuela.

Los estudiantes también se habían visto expuestos a ciberdelitos y otras actividades nocivas. Dejando a un lado los virus informáticos, más del 10 por ciento de los estudiantes encuestados había sufrido ciberacoso, mientras que el 25 por ciento había sido contactado por un desconocido en línea. El cuestionario también incluyó una sección dedicada a actos ilícitos o inadecuados, de la que se infirió que alrededor del 35 por ciento de los estudiantes había enviado mensajes mezquinos o dañinos que podrían considerarse constitutivos de ciberacoso. Aproximadamente el mismo número de estudiantes había intentado, o conseguido, entrar en una red inalámbrica protegida.

---

60 Documento 2/264 de la CE 2 del UIT-D de la Federación de Rusia.
61 Véase el Artículo 4 de la Ley Federal Nº 2124, https://digital.gov.ru/ru/documents/6406/ (disponible únicamente en ruso); Documento 2/264 de la CE 2 del UIT-D de la Federación de Rusia.
62 Documento SG2RGQ/135 de la CE 2 del UIT-D de Bhután.

Dadas las limitaciones de esa primera encuesta, Bhután llevó a cabo otra encuesta sobre seguridad y protección de la infancia en línea a nivel nacional. La encuesta formaba parte del proyecto "Digital Kids Asia Pacific" (DKAP), iniciado por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO Bangkok) con el apoyo del Korean Funds-in-Trust (KFIT). En ella participaron 2 381 estudiantes de entre 12 y 17 años, procedentes de 45 escuelas de todo el país, y se les plantearon 112 preguntas para conocer su nivel de conocimientos en materia de ciberseguridad, amenazas y medidas preventivas. El estudio reveló que la mayoría de los estudiantes (81 por ciento) tiene acceso a un teléfono inteligente en casa. Los estudiantes suelen pasar, por término medio, entre una y dos horas diarias en línea. Además, el 54 por ciento de los estudiantes carece de conocimientos para discernir la información fidedigna de la que no lo es. Asimismo, lo que más le preocupa al 49 por ciento de los estudiantes es que alguien haga un uso indebido de su información personal.

Son pocos los estudiantes (10 por ciento) que dan información falsa para eludir las restricciones de edad de las aplicaciones, que intimidan a otros con mensajes ofensivos o que entran en cuentas ajenas. Además, el 85 por ciento de los estudiantes no tiene reparos en hacer nuevos amigos por Internet y al 68 por ciento de los estudiantes no les importa hablar con personas de lugares u orígenes distintos a los suyos. El dato preocupante es que el 51 por ciento de los estudiantes se ha reunido alguna vez con desconocidos con quienes entraron en contacto en Internet y el 22,8 por ciento de estudiantes se declara abierto a la idea de reunirse con desconocidos en el futuro, siendo las mujeres más propensas a conocer a desconocidos que los varones.[63]

En Côte d'Ivoire, la PLCC llevó a cabo una encuesta a 200 jóvenes de tres institutos de Abiyán, a fin de analizar el comportamiento de los niños en línea, detectar los riesgos existentes y proponer estrategias de seguridad eficaces para combatir el abuso en línea.[64]

En total, el 83 por ciento de los encuestados declaró que utilizaba Internet. La razón principal por la que el porcentaje restante no utilizaba este recurso era el coste de los teléfonos inteligentes y los terminales. Para los niños de entre 15 y 18 años, la televisión había quedado relegada a un uso secundario, mientras que el 86,3 por ciento tenía una cuenta en un medio social. Este grupo de edad prefería acceder a Internet a través de un teléfono inteligente. Las imágenes y películas violentas se erigieron en la principal fuente de experiencias negativas en línea, seguidas por la piratería y, en último lugar, los insultos y las amenazas. En menor medida, los encuestados declararon haber tenido experiencias negativas con connotaciones sexuales. Algunos encuestados afirmaron haber sido chantajeados con vídeos explícitos en términos sexuales.

Según dicha encuesta, las experiencias que más daño pueden causar a los niños son:

- virus, errores, correos basura o actos de piratería (24 por ciento);
- vídeos sexuales (7,5 por ciento);
- imágenes o vídeos violentos (28,6 por ciento);
- uso de fotos sin acuerdo previo (7,5 por ciento);
- insultos, mezquindades o amenazas (19,5 por ciento);
- robo de identidad (6,7 por ciento);
- contacto con un desconocido (4,51 por ciento);

[63] Documento 2/385 de la CE 2 del UIT-D de Bhután.
[64] Documento 2/201 de la CE 2 del UIT-D de Côte d'Ivoire.

- estafas (0,75 por ciento); y
- extorsión sexual (0,75 por ciento).

Apoyo de la UIT a los Estados Miembros en relación con la protección de la infancia en línea

Del 4 al 6 de abril de 2018, en colaboración con la Academia Nacional de Telecomunicaciones de Odessa A. S. Popov, la UIT celebró un taller regional sobre ciberseguridad y protección de la infancia en línea para Europa y la Comunidad de Estados Independientes (CEI) en Odessa (Ucrania).[65] Las versiones finales de todos los documentos (incluidos el orden del día, los informes, las conclusiones y recomendaciones, la lista de participantes, las presentaciones y las fotografías) se publicaron en el sitio web de la academia[66] y en el de la UIT.[67] Los participantes en el taller, que actuaron en representación de 14 Estados Miembros, llegaron a la conclusión de que las regiones de Europa y la CEI debían reforzar su cooperación a fin de optimizar el uso de los recursos disponibles y lograr resultados prácticos, incluso mediante la traducción del material didáctico relacionado con la ciberseguridad y la protección de la infancia en línea. Las conclusiones y recomendaciones elaboradas por los participantes en el taller figuran en el documento de resultados.[68]

La protección de la infancia en línea es uno de los ejes principales de la iniciativa regional de la UIT para Europa sobre creación de confianza y seguridad en la utilización de las telecomunicaciones/TIC. En respuesta a aquellos Miembros que solicitaron hojas de ruta para las iniciativas de protección de la infancia en línea, la UIT llevó a cabo una encuesta entre los gobiernos nacionales incluidos en la iniciativa regional, en la que abordó una amplia gama de cuestiones relacionadas con las políticas y prácticas presentes en todas las plataformas tecnológicas que utilizan los niños y los jóvenes en el espacio digital. La encuesta se realizó por primera vez entre todos los Estados Miembros en 2009 y, en 2016, se divulgó una versión revisada de la misma entre los Estados Miembros de Europa Central y Oriental, la zona del Báltico y los Balcanes.

De acuerdo con las respuestas recibidas, la BDT publicó en 2017 un examen regional de las actividades nacionales en materia de protección de la infancia en línea en Europa, en el que especificó en qué punto se hallaban los países participantes en términos de desarrollo, adopción, aplicación y supervisión de las políticas atinentes a la protección de la infancia en línea.[69] En dicho examen incluyó ejemplos de prácticas vigentes en Albania, Bosnia y Herzegovina, Bulgaria, Chipre, Croacia, Estonia, Finlandia, Grecia, Hungría, Letonia, Liechtenstein, Lituania, Macedonia del Norte, Mónaco, Montenegro, Polonia, Eslovaquia, República Checa, Rumania, Serbia, Eslovenia y Turquía.

El Grupo de Trabajo del Consejo de la UIT sobre Protección de la Infancia en Línea (GTC-PIeL) lleva a cabo su labor conforme a lo estipulado en la Resolución 1306 (2009) del Consejo de la UIT,

---

65 Documento 2/75 de la CE 2 del UIT-D de la Academia Nacional de Telecomunicaciones de Odessa A.S. Popov (Ucrania).

66 Academia Nacional de Telecomunicaciones de Odessa A.S. Popov. Taller regional de la UIT sobre ciberseguridad y protección de la infancia en línea para Europa y la CEI, Odessa (Ucrania), 4-6 de abril de 2018.

67 UIT. Taller regional de la UIT sobre ciberseguridad y protección de la infancia en línea para Europa y la CEI, Odessa (Ucrania), 4-6 de abril de 2018.

68 UIT. Conclusions and reccomendations, Taller regional de la UIT sobre ciberseguridad y protección de la infancia en línea para Europa y la CEI, Odessa (Ucrania), 4-6 de abril de 2018.

69 UIT-D. Regional review of national activities on child online protection in Europe, 2017.

así como en la Resolución 179 (Rev. Dubái, 2018), en que la Conferencia de Plenipotenciarios resolvió que la UIT continuara con la iniciativa de Protección de la Infancia en Línea como plataforma para crear conciencia sobre las cuestiones relativas a la seguridad de la infancia en línea; siguiera brindando asistencia y apoyo a los Estados Miembros, en particular a los países en desarrollo, en la elaboración y aplicación de hojas de ruta relacionadas con la iniciativa; y siguiera coordinando la iniciativa, en cooperación con las partes interesadas pertinentes.[70]

La información relativa a la 15ª, 16ª y 17ª reunión del GTC-PIeL, celebradas el 26 de septiembre de 2019, el 4 de febrero de 2020 y el 26 de enero de 2021, respectivamente, en Ginebra y a distancia, se sometió a la consideración de la Cuestión 3/2.[71],[72]

Entre los documentos presentados en dichas reuniones figuran:

- una versión actualizada de las Directrices de la UIT sobre protección de la infancia en línea;[73]
- una presentación de los resultados de la consulta a los jóvenes en línea;[74]
- una presentación de la labor y las actividades de la UIT en materia de protección de la infancia en línea;[75]
- una presentación del proceso de revisión de las Directrices sobre protección de la infancia en línea 2019-2020;[76] y
- una presentación de la iniciativa de Protección de la Infancia en Línea de la UIT y de la aplicación de las Directrices sobre PIeL 2020.[77]

Uno de los principales resultados de las reuniones fue el reconocimiento de la necesidad de proporcionar orientaciones sobre formas de incrementar el número de respuestas de jóvenes y afianzar el compromiso y la participación de las partes interesadas en el GTC-PIeL, dada la importancia de evaluar la eficacia del programa.

En 2020, la UIT celebró una serie de foros temáticos[78] para propiciar un intercambio de experiencias relacionadas con la protección de la infancia en línea entre las distintas partes interesadas, dar a conocer las Directrices sobre protección de la infancia en línea y facilitar su promoción, adaptación y contextualización a escala nacional y regional:

- África: 30 de octubre de 2020;[79]
- Américas: 19 de octubre de 2020;[80]
- Estados Árabes: 23 de noviembre de 2020;[81]

---

70 UIT. Conferencia de Plenipotenciarios, Resolución 179 (Rev. Dubái, 2018), "Función de la UIT en la protección de la infancia en línea".
71 Documento SG2RGQ/242 de la CE 2 del UIT-D del Grupo de Trabajo del Consejo sobre Protección de la Infancia en Línea (GTC-PIeL).
72 Las contribuciones presentadas por los miembros y los expertos externos pueden consultarse en los siguientes enlaces: 15ª reunión, 16ª reunión, 17ª reunión.
73 UIT. GTC-PIeL, Documento CWG-COP-14/2, "Update on the ITU Child Online Protection (COP) Initiative".
74 UIT. GTC-PIeL, Documento CWG-COP-15/INF/3, "Youth Online Consultation".
75 UIT. GTC-PIeL, Documento CWG-COP-16/5, "ITU's work and activities in child online protection".
76 UIT. GTC-PIeL, Documento CWG-COP-16/4, "ITU Child Online Protection: COP Guidelines Review Process 2019-2020".
77 UIT. GTC-PIeL, Documento CWG-COP-17/2(Rev.1), "ITU COP 2020, Child online protection & empowerment".
78 UIT. Publicaciones regionales: Directrices PIeL 2020.
79 UIT-D. Publicación regional de las Directrices PIeL para África revisadas, 30 de octubre de 2020.
80 UIT-D. Directrices PIeL para las Américas, 19 de octubre de 2020.
81 UIT-D. Diálogo Regional en línea sobre las Directrices PIeL de la UIT 2020 y las oportunidades de implementación en la Región Árabe, 23 de noviembre de 2020.

- Asia y el Pacífico: 3 de noviembre de 2020;[82]
- Comunidad de Estados Independientes: 27 de octubre de 2020;[83]
- Europa: 26 y 27 de noviembre de 2020.[84]

3.3 Enseñanzas extraídas, próximos pasos, iniciativas y conclusiones

La necesidad de proteger a la infancia en línea ha adquirido un carácter especialmente acuciante durante la pandemia de COVID-19.

De las actividades de los Estados Miembros en ámbitos relacionados con la protección de la infancia en línea pueden colegirse diversas enseñanzas, entre las que cabe destacar las siguientes:

- cada país debe reconocer su responsabilidad de velar por que Internet y las tecnologías conexas sean seguras para los niños y los jóvenes;
- los países están integrando progresivamente la creación de conciencia sobre los riesgos en línea en los programas generales de protección de la infancia y crianza de los hijos;
- la idea de que Internet también puede contribuir a la promoción de la educación cívica y el aprendizaje está ganando terreno, no obstante, en muchos casos la escasez de recursos y conocimientos técnicos en el plano local parece frenar el desarrollo;
- aunque, en líneas generales, los marcos legislativos de muchos países se ajustan a los correspondientes instrumentos jurídicos internacionales y regionales, es sumamente importante que todos los países se aseguren de que sus medidas legales y su marco legislativo sigan el ritmo de los avances tecnológicos y la evolución conductual;
- los coordinadores nacionales ejercen una función esencial para garantizar una protección efectiva en línea, y todos los países deberían contar con un coordinador nacional que disponga de los recursos necesarios y participe en las iniciativas regionales e internacionales.[85]

También existen numerosas esferas en las que los Estados Miembros podrían facilitar aún más la puesta en marcha de actividades de protección de la infancia en línea, en especial:

- la concienciación y la formación en materia de alfabetización digital, tanto para los profesionales de la ciberseguridad como para los niños, los padres y los docentes;
- la elaboración de leyes y reglamentos a efectos de la protección de la infancia en línea;
- la realización de encuestas representativas para una mejor adecuación de las políticas, iniciativas y acciones existentes en relación con la protección de la infancia en línea.

Las asociaciones sin ánimo de lucro y las organizaciones comunitarias pueden tomar medidas encaminadas a la creación de conciencia y el desarrollo de competencias entre los niños, a fin de ayudarles a hacer un mejor uso de Internet en un entorno seguro. Algunas de estas medidas podrían consistir en:

- desdramatización de la prevención para no alentar la cultura del miedo que se ha impuesto entre los padres en relación con el uso que sus hijos hacen de Internet, evitando un enfoque que pueda agravar la ansiedad de los progenitores que ya recelan de una

---

82 UIT-D. Foro de Desarrollo Regional de la UIT para Asia y el Pacífico (FDR ASP), Post-forum Session on Cybersafety – Launching de 2020 Child Online Protection Guidelines for Asia and the Pacific, 3 de noviembre de 2020.

83 UIT-D. UIT-UNESCO IITE, Foro sobre la Protección de la Infancia en Línea en la Región de la CEI, 27 de octubre de 2020.

84 UIT-D. Foro de la UIT para Europa sobre la Protección de la Infancia en Línea, 26-27 de noviembre de 2020.

85 Documento SG2RGQ/47 de la CE 2 del UIT-D del Coordinador de la BDT para la Cuestión 3/2.

tecnología que no acaban de entender, saboteando así la extraordinaria herramienta de aprendizaje que es Internet;
- fomentar los programas educativos destinados a la definición de prácticas idóneas en materia de gestión de contenidos, y enseñar a los niños a utilizar Internet de forma responsable;
- crear un portal de Internet que proporcione a niños, adolescentes, padres y docentes una base educativa; e
- implicar a todas las partes interesadas en las actividades de sensibilización comunitarias, incluidos organismos gubernamentales, empresas de Internet, organizaciones no gubernamentales, grupos comunitarios y el público en general.[86]

En términos generales, puede concluirse que:

- la cooperación internacional y el apoyo estatal son esenciales para garantizar la ciberseguridad y la protección de la infancia en línea;
- en los países en desarrollo, cabría utilizar las herramientas políticas nacionales con el objetivo de elaborar estrategias de ciberseguridad;
- las asociaciones público-privadas son importantes para mejorar la eficacia de las herramientas de carácter organizativo y técnico que se aplican en favor de la ciberseguridad;
- tanto el desarrollo de nuevos mecanismos estratégicos y normativos para la protección de la infancia en línea, como la evaluación de los mecanismos existentes, han alcanzado un punto álgido;
- las instituciones educativas y las empresas privadas deberían participar en la ejecución de proyectos encaminados a la creación de herramientas organizativas y técnicas para la protección de la infancia en línea, incluso en el marco de las iniciativas regionales de la UIT;
- deben desarrollarse programas educativos y herramientas para la protección de la infancia en línea que tengan en cuenta las necesidades de los niños con discapacidad;
- los Estados Miembros deben revisar sus compromisos en relación con el Índice de Ciberseguridad Global (ICG) y emprender nuevas iniciativas; y
- las instituciones educativas, las entidades del sector privado y las organizaciones no gubernamentales deberían participar en las actividades del UIT-D, incluidos los trabajos de las Comisiones de Estudio de la UIT y los centros de excelencia que imparten cursos de formación sobre ciberseguridad.

A fin de elaborar soluciones más eficaces, es fundamental que todas las partes interesadas compartan información sobre las herramientas disponibles en el ámbito de la ciberseguridad y la protección de la infancia en línea, dada la creciente importancia de esta última a escala mundial y la necesidad de colaborar en ese sentido, especialmente en el marco de las actividades del UIT-D.[87]

[86] Documento 2/201 de la CE 2 del UIT-D de Côte d'Ivoire.
[87] Documento 2/75 de la CE 2 del UIT-D de Academia Nacional de Telecomunicaciones de Odessa A.S. Popov (Ucrania)

Capítulo 4 – Problemas de ciberseguridad para las personas con discapacidad

4.1 Introducción

Nadie está libre de sufrir un ciberataque. En ese sentido, las personas con discapacidad no deberían correr más ciberriesgos por una mera falta de información o concienciación.

Durante el periodo de estudios 2014-2017, la Comisión de Estudio 2 del UIT-D realizó una encuesta centrada en la sensibilización sobre la ciberseguridad, cuyos resultados se publicaron en un informe final.[88] Dicha encuesta reveló que las personas de edad avanzada y las personas con discapacidad eran los dos grupos en los que menos reparaban las campañas de concienciación sobre ciberseguridad. Además, el 69 por ciento de los Estados Miembros que participaron en la encuesta no incluyó a las personas con discapacidad entre los grupos destinatarios de sus campañas de sensibilización en materia de ciberseguridad.

Los resultados muestran claramente que es preciso ahondar en esta cuestión. Con el objetivo de crear conciencia sobre las necesidades específicamente relacionadas con la ciberseguridad de las personas con discapacidad y otras partes interesadas, incluidos gobiernos y organizaciones privadas, la Cuestión 3/2 ha seguido examinando aspectos atinentes a la seguridad y cibervulnerabilidades partiendo de una serie de casos de uso. En este capítulo se exponen los casos de uso, las enseñanzas extraídas y otros datos útiles.

4.2 Casos de uso

4.2.1 Remitentes de mensajes basura e impostores cuyo objetivo son las personas con discapacidad

Consideraciones generales

Las personas que envían mensajes basura y las que se apropian indebidamente de direcciones de correo electrónico utilizan métodos cada vez más sofisticados y han desarrollado la capacidad no solo de saber si un posible objetivo tiene una discapacidad, sino también de utilizar esa discapacidad para hacerse pasar por el objetivo en cuestión. Las personas con discapacidad también afrontan obstáculos para obtener ayuda de los departamentos de seguridad y fraude de sus proveedores de correo electrónico.

Las personas con discapacidad están en el punto de mira de este tipo de infractores, que se hacen pasar por su objetivo utilizando la discapacidad de la persona en cuestión como medio

[88] UIT. Informe final de la Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D para el periodo de estudios 2014-2017, Seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad. UIT, 2017.

de identificación. Uno de los casos estudiados versa sobre la apropiación indebida de la cuenta de correo electrónico de una persona sorda que se comunicaba en lengua de señas. Aunque en este caso la víctima tenía una cuenta de Gmail, podría haberse tratado de cualquier proveedor de cuentas de correo electrónico. Desgraciadamente, el servicio de asistencia de Gmail fue de poca ayuda. Una vez que la víctima abrió el enlace fraudulento, el remitente del mensaje basura se apropió de su cuenta, obteniendo así acceso a su lista de contactos y, posiblemente, a otros archivos de su ordenador.

En última instancia, el servicio de asistencia le dijo a la víctima que la única solución era cambiar de proveedor y de dirección de correo electrónico. Aunque en este caso la persona afectada era sorda, no es descabellado pensar que los atacantes puedan utilizar cualquier discapacidad para perpetrar este tipo de robo de identidad.

Es importante que los usuarios de correo electrónico, incluidos los usuarios con discapacidad, comprendan la importancia de verificar todos los enlaces que reciben, incluso de amigos, antes de abrirlos. Los servicios de asistencia de los proveedores de correo electrónico también deben interesarse vivamente por esta forma de abuso, especialmente cuando el blanco son comunidades vulnerables. En este caso, la víctima llamó al número de teléfono del servicio de asistencia con la ayuda de un amigo o de un servicio de transmisión telefónica para personas sordas. Los proveedores de servicios deberían tramitar este tipo de llamadas con más seriedad o proporcionar un número de teléfono especial atendido por teleoperadores con los que los usuarios sordos puedan comunicarse directamente utilizando un teletipo. Preferible sería que los proveedores de servicios contrataran a teleoperadores que dominasen la lengua de señas. En los Estados Unidos, empresas de la índole de Amazon ya han tomado medidas para ofrecer estos servicios.

Ejemplos de correos electrónicos

A continuación, figuran dos ejemplos del tipo de correo electrónico que el infractor del caso descrito *supra* envió a la lista de contactos de la víctima. En respuesta, la víctima informó a sus contactos de que su cuenta había sido pirateada y cambió de proveedor de correo electrónico.

Ejemplo 1: *El remitente del mensaje basura se hace pasar por la persona con discapacidad*.

De: Persona con discapacidad personacondiscapacidad@gmail.com
Enviado: 23 de marzo de 2018 13.00
Asunto: ¡¡INCREÍBLE!! El país X AUMENTA LA PRESTACIÓN MENSUAL PARA PERSONAS SORDAS EN UN 70 por ciento

¡Increíble! En consideración a todas las personas sordas y con audición reducida, el Presidente del país "X" ha decidido aumentar la prestación de la seguridad social/ el ingreso de seguridad suplementario y el seguro de discapacidad de la seguridad social en un 70 por ciento. Esta es una buena noticia para todas las personas sordas y con audición reducida del país X.

Para obtener más información y saber cuánto aumentará su prestación, visite el siguiente enlace:

http://noisecancel.net/js/gggg/G/G/us/index .php

[Nota: El enlace fraudulento original se ha modificado.]

Acceda con su dirección de correo electrónico y compruebe que todos los datos son correctos.

DeafNews

Ejemplo 2: *La víctima comunica a sus contactos que su cuenta ha sido pirateada.*

¡Hola a todos!

Como ya sabéis, hace tres semanas me enviaron un enlace interesante a un vídeo en ASL y, al abrirlo, ¡me piratearon mi antigua cuenta de Gmail!

[Nota: ASL significa *American Sign Language* o lengua de señas estadounidense].

El infractor sigue enviando correos electrónicos FALSOS utilizando mi cuenta de Gmail. Lo que me preocupa es que el contenido parece real y aparenta estar vinculado a las actividades que desempeño como persona sorda.

Tras haber pasado horas buscando en Google, encontré un número de teléfono, el (855) 836-3987, para contactar con un operador.

¿Y sabéis qué pasó? Que, en lugar de intentar ayudarme, me contestaron "qué pena".

¿Es segura tu cuenta de Gmail?

Mientras tanto, elimina CUALQUIER correo electrónico.

<de personacondiscapacidad@gmail.com>

Mis más sinceras disculpas,

Persona con discapacidad

Enseñanzas extraídas y mejores prácticas propuestas

- La comunidad de personas con discapacidad debería recibir información sobre los problemas que se sabe conllevan los mensajes basura y los programas maliciosos.
- Los proveedores de servicios deberían contar con personal capacitado para atender consultas de clientes con discapacidad.
- Los usuarios de correo electrónico no deberían abrir ningún enlace a ningún sitio web sin verificar antes la fuente.
- Las víctimas de una apropiación indebida de correo electrónico deberían:
    - informar a su proveedor de servicios de correo electrónico;
    - reenviar el correo electrónico sospechoso a la sección de fraudes del proveedor de correo electrónico;
    - solicitar el bloqueo de la dirección de correo electrónico objeto de apropiación;
    - cambiar de dirección de correo electrónico;
    - informar a todos sus contactos de que la dirección de correo electrónico en cuestión ha sido pirateada y facilitarles la nueva dirección.

4.2.2 Ciberriesgos asociados a las tecnologías de apoyo basadas en la IoT

Antecedentes

Según la Organización Mundial de la Salud (OMS), más de 2 000 millones de personas tienen algún tipo de discapacidad, lo que constituye el 37,5 por ciento de la población mundial.[89] De acuerdo con el Departamento de Asuntos Económicos y Sociales de las Naciones Unidas, los países no comparten una definición común del término "persona con discapacidad" y, en consecuencia, han adoptado una amplia gama de clasificaciones y umbrales.[90] Según la definición aceptada por la OMS a escala internacional, son personas con discapacidad aquellas que adolecen de problemas que afectan a una estructura o función corporal, de limitaciones de la actividad o de dificultades para ejecutar una tarea o llevar a cabo una acción.[91]

Tal como se desprende de esta definición, existen muchos tipos de discapacidad. Cada discapacidad conlleva una barrera en la vida de la persona afectada. No obstante, la tecnología está desempeñando un papel importante en la eliminación de estas barreras y la mejora de las condiciones de vida de las personas con discapacidad.

Actualmente, la tecnología se ha generalizado e influye tanto en la vida cotidiana de las personas como en la sociedad en su conjunto. A lo largo del último decenio, la IoT ha demostrado el potencial que alberga como herramienta de mejora de las condiciones de vida de las personas con discapacidad.[92] Por tanto, las tecnologías de apoyo basadas en la IoT son un recurso cada vez más utilizado a efectos de la superación de las limitaciones derivadas de las discapacidades.[93]

En la Convención sobre los derechos de las personas con discapacidad, las TIC se consideran una herramienta esencial para las personas con discapacidad. En particular, en el Artículo 9, relativo a la accesibilidad, se destaca el papel de las TIC en la promoción de la independencia y la plena participación de las personas con discapacidad en diferentes ámbitos y se encomienda a los Estados Parte que realicen esfuerzos conjuntos y conscientes en pro del acceso a las TIC[94].

Tanto las TIC como la IoT obran en favor de la seguridad, la movilidad y la independencia. En ese sentido, se han concebido numerosos dispositivos y servicios de IoT para mejorar las condiciones de vida y reducir la dependencia de las personas con discapacidad, véanse desde prótesis conectadas a Internet hasta zapatos inteligentes que vibran para guiar al usuario.[95] Por ejemplo, las personas ciegas o con deficiencia visual pueden utilizar la tecnología para orientarse en su entorno y acceder a información escrita. Además, las tecnologías domésticas inteligentes permiten a los usuarios controlar los electrodomésticos y otros dispositivos de sus hogares a los que puede ser difícil acceder, como luces, cerraduras y sistemas de seguridad.

---

89 OMS. Informe mundial sobre la discapacidad 2011. OMS 2011.
90 Departamento de Asuntos Económicos y Sociales de las Naciones Unidas (UNDESA). Disability and Development Report: Realizing the Sustainable Development Goals by, for and with persons with disabilities. Naciones Unidas, Nueva York, 2018.
91 OMS. *Op. cit.*, Capítulo 1.
92 Future of Privacy Forum. The Internet of Things (IoT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions, enero de 2019.
93 OMS. Health topics. Assistive technology.
94 UNDESA. Convención sobre los derechos de las personas con discapacidad (CSPD). Artículo 9 – Accesibilidad.
95 Future of Privacy Forum. *Op. cit.*

La tecnología: Un arma de doble filo

A pesar de las numerosas ventajas que ofrecen, las tecnologías de apoyo basadas en la IoT también elevan proporcionalmente el nivel de exposición de los usuarios a los ciberriesgos. Dada la creciente dependencia de las tecnologías de apoyo, cualquier interrupción o alteración de estas últimas podría conllevar un aumento de la vulnerabilidad.

A menudo, los dispositivos y servicios de IoT se caracterizan por unos niveles de seguridad subóptimos. Por ejemplo, algunos de ellos no utilizan sistemas de cifrado adecuados para la transmisión de los datos, lo que puede conducir a una divulgación indebida o a una fuga de los mismos. En el caso de las personas con discapacidad, los datos personales pueden ser especialmente delicados, ya que pueden revelar detalles de la condición médica del individuo.

Dada la importancia que revisten las tecnologías de apoyo para las personas con discapacidad, los ciberriesgos pueden entrañar unas consecuencias catastróficas. Por ejemplo, algunas personas con discapacidad física dependen de prótesis biomecánicas para recuperar total o parcialmente la capacidad de movimiento. Estas prótesis utilizan sensores específicos para leer y analizar parámetros de contracción muscular, a fin de reproducir distintos movimientos a través de los dispositivos (por ejemplo, para mover los dedos de un brazo protésico). Las prótesis envían regularmente datos a la nube, para fundamentar su capacidad de análisis computacional y mejorar su eficacia. A causa de esta relación de conectividad, los dispositivos en cuestión pueden sufrir ataques destinados a acceder a los datos incluidos en la nube, manipularlos o borrarlos, o a acceder a los datos personales de los usuarios. Además, los atacantes pueden tomar el control de las prótesis a distancia. Si la prótesis está conectada a un implante cerebral, las consecuencias podrían ser aún peores.[96]

También podría citarse el ejemplo de las personas con problemas de audición que dependen de implantes cocleares más invasivos que los audífonos estándar. Esta tecnología se basa en tres componentes básicos: un micrófono, un procesador de voz y un receptor-estimulador implantado. Algunos implantes cocleares modernos van acompañados de dispositivos de control remoto que permiten a los usuarios modificar los ajustes del implante a través de una aplicación móvil. Un ataque básico podría consistir en apagar el implante para dejar a la víctima sorda. Los ataques más sofisticados podrían centrarse en impedir que el procesador de voz reciba el estímulo del micrófono o en alterar el receptor para que transmita los sonidos generados por el atacante. Los ataques más sofisticados podrían ser más difíciles de detectar, especialmente en los casos en que los usuarios de los implantes cocleares carecen de medios alternativos para verificar lo que oyen.

Además de a las tecnologías de apoyo, los infractores también pueden dirigir sus ataques a otras tecnologías de uso común entre personas con discapacidad. Por ejemplo, las personas con deficiencia visual perderían todo medio de navegación fiable si sus herramientas GPS fallasen o fueran deliberadamente manipuladas por un atacante. En los ataques de falsificación GPS, se sitúa un transmisor radioeléctrico cerca del objetivo para interferir con la señal GPS legítima.[97] A continuación, el atacante puede transmitir coordenadas imprecisas o interrumpir la transmisión de datos, lo que puede conllevar daños físicos o tener otras repercusiones graves.

---

[96] *Vladimir Dashchenko*, How to Attack and Defend a Prosthetic Arm. Securelist (Kaspersky), 26 de febrero de 2019.

[97] Maria Korolov, What is GPS spoofing? And how you can defend against it, *sitio web CSO*, International Data Group (IDG), 7 de mayo de 2019.

Aunque estos son solo algunos ejemplos de los ciberataques que pueden sufrir las tecnologías digitales de apoyo, bastan para poner de manifiesto la importancia de la ciberseguridad para la seguridad de las personas con discapacidad que dependen de estas tecnologías.

Próximos pasos que pueden considerarse

Internet y la IoT pueden facilitar la participación social, económica y civil de las personas con discapacidad. Aunque el potencial que albergan estas tecnologías es innegable, deben realizarse esfuerzos constantes para avenir los factores sociales, legislativos, personales y de infraestructura en el ecosistema de la IoT, de tal manera que se otorgue prioridad a la seguridad de los dispositivos de IoT. Los gobiernos podrían adoptar ciertas medidas concretas a fin de mejorar la seguridad y, en consecuencia, la fiabilidad de las tecnologías de apoyo.

Los gobiernos podrían adoptar medidas encaminadas a la mejora de la legislación y la política en materia de accesibilidad y seguridad de la IoT y a la creación de mecanismos para promoverlas y velar por su cumplimiento. Estos marcos deben partir de una evaluación de las necesidades de las personas con discapacidad y comprender una serie de funciones y responsabilidades bien definidas. Dada la probabilidad de que en este tema trabajen representantes de diversas esferas gubernamentales (por ejemplo, tecnología y telecomunicaciones, bienestar y medicina), la colaboración reviste una importancia crucial y debería promoverse en todas las iniciativas.

Podrían concebirse iniciativas específicas. Por ejemplo, los gobiernos podrían desarrollar sistemas de certificación en materia de ciberseguridad para las tecnologías de apoyo, que incluyeran pruebas y controles de seguridad periódicos, así como la obligación de realizar actualizaciones regulares del sistema para adaptarlo a la evolución tecnológica. Los gobiernos también podrían apoyar a los fabricantes concediéndoles incentivos, fomentando las asociaciones público-privadas y ofreciendo fondos para iniciar proyectos y subvenciones destinadas a la investigación y el desarrollo.

Asimismo, es necesario promover una cultura de seguridad que responda a los riesgos que conllevan estas tecnologías. Los gobiernos deberían colaborar con el sector privado en la realización de campañas de cibersensibilización dirigidas a la población.

En conclusión, aunque las tecnologías de apoyo basadas en la IoT brindan una asistencia fundamental a las personas con discapacidad, también entrañan una serie de riesgos que, si no se abordan adecuadamente, pueden tener graves consecuencias. Por consiguiente, las tecnologías de apoyo deben observar las más estrictas normas de seguridad y adaptarse a la evolución tecnológica.

Enseñanzas extraídas y mejores prácticas propuestas

Según se indica en los párrafos anteriores, conviene adoptar medidas de ciberseguridad para las personas con discapacidad, especialmente aquellas con dificultades auditivas, incluidos servicios de retransmisión de telecomunicaciones y subtitulado a distancia, a fin de mejorar la accesibilidad de los servicios de información y comunicación.

4.2.3 Examen de los aspectos relativos a la seguridad de los servicios de accesibilidad de las TIC

Introducción

Los servicios de accesibilidad de las TIC, entre ellos los de retransmisión de telecomunicaciones y subtitulado a distancia, ayudan a las personas con discapacidad a comunicarse y acceder a la información. Evidentemente, estos servicios exigen la adopción de medidas para proteger la seguridad y la privacidad de las personas con discapacidad y mitigar la cibervulnerabilidad de este y otros grupos de personas con necesidades específicas, como los niños y las personas de edad avanzada.

Aspectos relativos a la seguridad del subtitulado a distancia

El subtitulado a distancia es un servicio que consiste en transcribir las palabras pronunciadas en una reunión o conferencia en un lugar distinto al de celebración del evento.[98] En este caso, se utilizan servicios de TIC tales como teléfonos fijos, teléfonos móviles o micrófonos de ordenador, para enviar la voz del orador al subtitulador, que se encarga de transcribir la voz a texto. El texto transcrito se transmite en tiempo real al lugar de celebración del evento, donde puede leerse. El texto subtitulado a distancia suele mostrarse en una pantalla o un monitor público, situado en la sala de reunión, o en una pantalla personal. Los servicios de subtitulado a distancia no solo son esenciales para que las personas sordas o con dificultades de audición puedan participar en las reuniones, sino que también son útiles para aquellas cuya lengua materna no es la utilizada en la reunión, o incluso para situaciones en las que oradores con voces y acentos diversos participan en varios grupos (por ejemplo, en el lugar de trabajo, en un aula o en salones comunitarios). La persona que realiza las transcripciones para un servicio de subtitulado a distancia, denominada "subtitulador", debe estar cualificada como redactor de actas literales. El subtitulador también suele denominarse "relator de voz a texto".

Diversos códigos de prácticas nacionales y locales exigen la prestación de servicios de subtitulado a distancia. El proveedor debe tomar todas las medidas de precaución razonables para garantizar la privacidad de la reunión, en la que puede compartirse información confidencial.

Tipos de información confidencial

A continuación figura una lista no exhaustiva de posible información confidencial:

- información sensible discutida en reuniones y/o conferencias;
- datos médicos de pacientes;
- información jurídica sobre personas físicas;
- sesiones de asesoramiento; e
- información sobre el cumplimiento de la normativa de protección de datos.

[98] Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T), Documento Técnico FSTP-ACC-RCS, "Overview of remote captioning services", 17 de octubre de 2019.

Los proveedores de servicios de subtitulado a distancia deben observar las leyes y los reglamentos aplicables en materia de privacidad y protección de datos, entre ellos los establecidos por la Unión Europea.[99]

Cifrado del texto subtitulado

El texto transmitido en continuo a una pantalla o un terminal personal debería estar protegido por una contraseña. El proveedor de servicios de subtitulado a distancia es responsable de la seguridad del texto y está obligado a cumplir los requisitos de protección de datos pertinentes. Se recomienda encriptar el texto y, en su caso, la URL de la fuente utilizando el protocolo de capa de conexión segura (secure sockets layer) u otra tecnología aplicable.

Cifrado de audio

Los datos de audio originales del evento deben estar firmemente protegidos.

Aspectos relativos a la seguridad de los servicios de retransmisión de telecomunicaciones

Equivalencia funcional

La equivalencia funcional se traduce en que las personas con distintas capacidades (en particular las personas con discapacidad y con necesidades específicas) puedan utilizar un servicio o sistema de comunicación con una gama de funciones y un nivel de comodidad análogos a los ofrecidos al grupo más amplio de usuarios de una población. Este concepto abarca aspectos técnicos y económicos y parte del principio de no discriminación financiera de los usuarios de los servicios de retransmisión.[100]

La equivalencia funcional comprende los requisitos en materia de seguridad aplicables a los proveedores de servicios de comunicación en cualquier jurisdicción. Además, supone que los usuarios de los servicios de retransmisión deben gozar de los mismos derechos que los demás usuarios de la comunidad, especialmente en lo que respecta a los tipos de llamadas que permiten los servicios de retransmisión, lo que puede repercutir en su seguridad.

Requisitos de seguridad aplicables a la equivalencia funcional

A fin de lograr la equivalencia funcional, es esencial garantizar la confidencialidad, la privacidad y la seguridad de los servicios de retransmisión telefónica, las tecnologías que utilizan estos últimos y los teleoperadores que trabajan para ellos.

Los requisitos en materia de confidencialidad y seguridad de las llamadas de los servicios de retransmisión telefónica, incluida la codificación, deberían ser acordes a los aplicables a los servicios de telecomunicaciones generales del país o la región en cuestión.

---

99 Unión Europea, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

100 UIT-T. Recomendación UIT-T F.930, "Multimedia telecommunication relay services".

Aspectos relativos a la cibervulnerabilidad de las personas con necesidades específicas

El hecho de garantizar una utilización segura de Internet reviste una importancia particular para las personas con discapacidad y los grupos con necesidades específicas, en especial las personas de edad avanzada y los niños. La reducción de la cibervulnerabilidad de estas comunidades es un objetivo urgente e importante, cuyo logro pasa por la elaboración y el cumplimiento de directrices.

4.3 Información útil

La Cuestión 7/1 de la Comisión de Estudio 1 del UIT-D trata del "acceso a los servicios de telecomunicaciones/TIC para las personas con discapacidad y con necesidades especiales" y aborda varios temas dentro de esta esfera.[101]

El grupo *Future of Privacy Forum* publica un informe titulado "The Internet of Things (IoT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions".[102]

Puede obtenerse más información al respecto en los documentos mencionados.

[101] Comisión de Estudio 1 del UIT-D. Cuestión 7/1.
[102] Future of Privacy Forum. *Op. cit.*

Capítulo 5 – Situación de los retos en materia de ciberseguridad, incluidos los asociados a tecnologías incipientes como la IoT y la computación en la nube

5.1 Introducción

El gran aumento de la capacidad tecnológica ha fomentado la digitalización en un mundo cada vez más unido e interconectado. Según el Foro Económico Mundial, ya ha dado comienzo la "Globalización 4.0", etapa en la que los activos y servicios digitales constituyen el elemento fundamental de la economía y las exportaciones.[103]

La innovación está transformando el panorama tecnológico a tenor de las nuevas necesidades empresariales y operacionales. La utilización de dispositivos de IoT y de la tecnología 5G es cada vez más generalizada, y se estima que para 2025[104] habrá 41 600 millones de dispositivos conectados en todo el mundo. Las soluciones de computación en la nube han pasado a ser primordiales en el plano operacional, puesto que el 94 por ciento de las empresas de todo el mundo dependen de ellas.[105] Habida cuenta de disponibilidad y precisión de los datos cada vez mayores, la inteligencia artificial permite asimismo desarrollar aplicaciones más avanzadas.

No obstante, el surgimiento de nuevas tecnologías trae consigo una mayor necesidad de ciberseguridad. La innovación digital ha permitido el desarrollo de nuevos productos, de mayor grado de sofisticación, lo que aumenta la probabilidad de que existan vulnerabilidades y deficiencias susceptibles de poder explotarse.

Las ciberamenazas son cada vez mayores. En 2018, se produjeron 80 000 ciberataques diarios, lo que constituye más de 30 millones de ataques por año.[106] En 2019, se registraron más de 90 000 millones de intentos diarios de acceder a información de carácter privado.[107] Las ciberamenazas son asimismo cada vez más sofisticadas y afectan a la economía digital de todo el mundo, en particular los sistemas ciberfísicos de hogares, ciudades inteligentes, vehículos, sistemas de producción e infraestructuras esenciales. Los expertos han demostrado que

---

103 Klaus Schwab, Globalization 4.0 – What Does It Mean? Foro Económico Mundial, 5 de noviembre de 2018.
104 Business Wire, The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast, 18 de junio de 2019.
105 Kim Weins, Cloud Computing Trends: 2019 State of the Cloud Report, Flexera Blog, 21 de mayo de 2020.
106 PurpleSec, 2019 Cyber Security Statistics Trends & Data: The Ultimate List of Cyber Security Stats, *PurpleSec* (blog), consultado el 27 de abril de 2020.
107 Check Point, Prepare for a New Cyber Cold War in 2020, Warns Check Point, comunicado de prensa, 24 de octubre de 2019.

también es posible acceder ilegítimamente a dispositivos médicos implantados en el cuerpo humano, por ejemplo marcapasos y bombas de insulina.[108]

Ese aumento de los ataques también obedece a la proliferación, a través de la web oscura, de la piratería informática como un servicio que se ofrece, con frecuencia, por un precio asequible. La ciberdelincuencia es cada vez más frecuente en el plano comercial y ha pasado a constituir un amplio mercado en el que los piratas informáticos venden una gran variedad de herramientas y servicios destinados a fines maliciosos, incluidos el robo de contraseñas de bajo nivel y la utilización de tecnologías muy sofisticadas de ataque y explotación, en particular, para perpetrar ataques de denegación de servicio distribuida (DDoS), utilizar programas maliciosos, extorsionar por medios informáticos y usar programas espía.[109] Por otro lado, las tecnologías incipientes, que a menudo se utilizan para mejorar las soluciones de ciberdefensa, pueden utilizarse de forma maligna para aumentar la eficacia y el alcance de las herramientas de pirateo informático.[110] La inteligencia artificial, las redes de bots automatizadas, la IoT y las soluciones de computación en la nube son cada vez más frecuentes en los ciberataques a gran escala, y la utilización de nuevas técnicas de pirateo informático, por ejemplo, las herramientas de suplantación de identidad automatizadas, con tecnologías incipientes ha aumentado el riesgo informático.

Un reto relevante a los efectos de ciberseguridad es la escasez general de competencias profesionales y la falta de concienciación de los empleados. A medida que aumenta el grado de sofisticación de las ciberamenazas, las organizaciones tienen más dificultades para contratar expertos en ciberseguridad capacitados para proteger sus sistemas.[111] En 2017, el 82 por ciento de los empleadores señalaron que su personal contaba con competencias de ciberseguridad inadecuadas. Se prevé que en 2021, 4 millones de puestos de trabajo sobre ciberseguridad queden sin cubrir.[112] Además, por lo general, el personal demuestra poca concienciación en materia de ciberamenazas. El factor humano desempeña un papel clave en la ciberseguridad y ha demostrado constituir un factor de riesgo relevante. En 2018, un estudio reveló que el 99 por ciento de los incidentes digitales fueron iniciados involuntariamente por empleados que fueron víctimas de procesos de ingeniería social, al tiempo que solo el uno por ciento obedeció exclusivamente a fallos o explotaciones de índole tecnológica.[113]

La ciberseguridad es una esfera en constante evolución, y las organizaciones deben revisar continuamente su situación en materia de ciberseguridad frente a las nuevas amenazas. Con objeto de lograr un entorno más seguro, conviene que las partes interesadas reflexionen sobre la gestión de los riesgos de ciberseguridad y privacidad; también conviene verificar, complementar y mejorar los procesos de gestión de riesgos de ciberseguridad y de protección de la privacidad, e identificar los aspectos clave de ciberseguridad y privacidad propios de soluciones y entornos tecnológicos específicos. En este capítulo se analizan muchas amenazas de ciberseguridad asociadas a tecnologías incipientes como la IoT, la computación en la nube, las redes 5G, la IA y la cuarta revolución industrial ("Industria 4.0"). También se reseñan las

---

108 Lily Hay Newman, These Hackers Made an App That Kills to Prove a Point, *Wired*, 16 de julio de 2019; Dan Goodin, Insulin Pump hack delivers fatal dosage over the air, *The Register*, 27 de octubre de 2011.
109 Armor, The Dark Market Report: The New Economy, 28 de septiembre de 2020.
110 Deloitte, Protecting against the changing cybersecurity risk landscape: Future of risk in the digital era, Deloitte&Touche LLC, 2019.
111 William Crumpler y James A. Lewis, The Cybersecurity Workforce Gap, Center for Strategic and International Studies, 29 de enero de 2019.
112 Rob Saunders. 134 Cybersecurity Statistics and Trens for 2021. Varonis. Actualizado el 16 de marzo de 2021.
113 Proofpoint, Proofpoint's Annual Human Factor Report Details Top Cybercriminal Trends: More than 99 Percent of Cyberattacks Need Humans to Click, 9 de septiembre de 2019.

tendencias actuales y los retos en relación con las amenazas que podrían menoscabar las ventajas de la innovación digital, incluidas posibles soluciones al respecto.

5.2 Amenazas de ciberseguridad, partes interesadas y motivos

El objetivo de las ciberamenazas es menoscabar los tres objetivos tradicionales de la ciberseguridad, a saber, la confidencialidad, la integridad y la disponibilidad. La confidencialidad restringe el acceso a la información únicamente a las personas autorizadas. La integridad garantiza la exactitud y la fiabilidad de la información y evita las alteraciones no autorizadas de los datos. Por último, la disponibilidad se refiere a la capacidad de acceder a datos e información cuando se necesita.

Las ciberamenazas son de índole muy diversa, y las llevan a cabo actores que persiguen objetivos de características y alcance diferentes. Por lo general, las personas que perpetran acciones malignas pueden ser:

- ***Personal interno***: según informes recientes, alrededor del 40 por ciento de los incidentes son provocados por personal interno, a menudo empleados descontentos que buscan venganza contra sus empleadores.[114] Pueden ser particularmente peligrosos, al tener acceso directo a datos, información y activos digitales.
- ***Activistas-piratas informáticos***: son personas motivadas por causas políticas y sociales. Suelen robar y difundir información confidencial con el objetivo de poner en riesgo a líderes políticos o a celebridades, y revelan datos confidenciales o clasificados en nombre de la libertad de expresión. También suelen alterar sitios web y realizar ataques DDoS contra determinados servicios o sitios web.[115]
- ***Ciberdelincuentes***: son delincuentes motivados por el beneficio económico. Hacen hincapié en información relativa a individuos, empresas y organizaciones con el objetivo de sacar beneficio económico. Suelen chantajear a sus víctimas, divulgar y vender datos e información de propiedad intelectual en mercados ilícitos y extorsionar por medios informáticos. Como se ha mencionado anteriormente, la ciberdelincuencia ha pasado a ser un servicio en el que varios grupos venden bienes y servicios para perpetrar ataques, que incluyen utilización ilegítima de sistemas y ciclos de ataques íntegros.
- ***Amenazas persistentes avanzadas* (APT)**: según la definición del Instituto Nacional de Normas y Tecnología de Estados Unidos (NIST), este tipo de amenazas proviene de adversarios muy sofisticados con muchos recursos y capacidad para acceder a redes de sus víctimas para revelar información, mermar o dificultar sistemas esenciales de dichas víctimas, o menoscabar sus activos digitales.[116] Estas amenazas se adaptan a los sistemas de defensa de las víctimas mediante múltiples vectores de ataque, y son capaces de perseguir su objetivo de forma sigilosa durante largos periodos de tiempo. Este tipo de ataques son los más sofisticados en términos de competencias técnicas, financiación y organización, y con frecuencia los patrocinan Estados, a tenor de intereses geopolíticos.

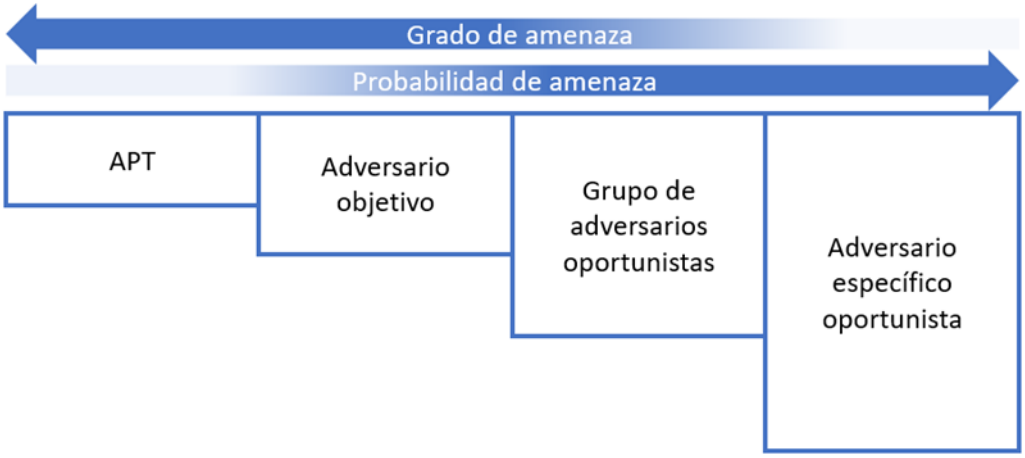
Pese a que todos los actores maliciosos tienen como objetivo poner en riesgo la confidencialidad, integridad y disponibilidad de información y activos, la intrusión en redes puede llevarse a cabo de varias formas. El término "ciberataque" abarca varias acciones, por ejemplo, la alteración de sitios web o los ataques de denegación de servicio, o ataques más graves como la destrucción de datos y sistemas esenciales mediante ataques con armas.

---

114 Verizon, 2019 Data Breach Investigations Report, Verizon, 2019.
115 Lillian Ablon, Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data, RAND Corporation, 2018.
116 NIST. Joint Task Force Transformation Initiative, NIST Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View, marzo de 2011.

Los actores maliciosos y sus ataques difieren en términos de sofisticación, duración y perjuicios causados. Aunque es imposible defenderse de todas las amenazas, las organizaciones pueden tener en cuenta varios modelos de amenazas para identificar las amenazas pertinentes con arreglo a su perfil, riesgo y contexto. En la **Figura 1** se muestra un modelo general de ciberamenazas, que pone de manifiesto que la mayoría de las organizaciones suelen hacer frente a amenazas específicas menos sofisticadas, de ahí que requieran medidas de protección menos articuladas.

Figura 1 – Modelo de amenaza



No obstante, las grandes empresas, las organizaciones que operan en sectores críticos estratégicos y las personas que gestionan información y activos valiosos, son más propensos a ser víctimas de ataques por amenazas específicas, o amenazas persistentes avanzadas.

En esta sección se ha proporcionado una visión general de las ciberamenazas. En el resto del capítulo se proporcionará información sobre la forma de aplicar esas amenazas a las tecnologías incipientes, y las estrategias, los marcos y las soluciones que cabe aplicar para hacer frente a las mismas.

5.2.1 Amenazas en el plano tecnológico

Las tecnologías incipientes permiten recabar, compartir, almacenar y analizar una gran cantidad de datos, a menudo a una velocidad sin precedentes. No obstante, sus características específicas, en particular su gran conectividad y la complejidad de los entornos en los que interactúan, pueden plantear una serie de retos tecnológicos y de organización para garantizar la seguridad.

Virtualización

La virtualización constituye un elemento fundamental de los entornos tecnológicos modernos, al permitir a los desarrolladores personalizar las infraestructuras para satisfacer las necesidades de las aplicaciones de red y apoyar el desarrollo de nuevas arquitecturas y protocolos en un entorno idóneo.[117] Sin embargo, la compartición de canales de comunicación y de dispositivos

[117] Leonardo Richter Bays *et al.*, Virtual network security: threats, countermeasures, and challenges, *Journal of Internet Services and Applications* 6, article N° 1 (2015).

de encaminamiento en situaciones de multidivisión plantea diversos riesgos de seguridad, en particular:[118]

- El riesgo de divulgación no autorizada de datos, tanto intencionada como no intencionada, se ve exacerbada en los entornos virtuales en los que los recursos físicos se comparten entre varios clientes o usuarios. Actividades malignas como la interceptación y el "scavenging" (búsqueda de residuos de datos en una red para adquirir información) pueden llevarse a cabo más fácilmente si el sistema permite la inspección cruzada de varios usuarios.
- La multidivisión puede aumentar los riesgos asociados a la cadena de suministro y dificulta la protección frente a intrusiones. Los atacantes pueden adquirir privilegios y acceder ilegítimamente a la red de su objetivo mediante recursos con un nivel de protección inferior que comparten la misma capa física como vector.
- En los entornos virtualizados, los resultados de la gestión de identidades son especialmente complejos, debido a los sistemas altamente jerarquizados de administración de privilegios. Ese contexto facilita la labor de actores maliciosos para realizar fraudes de identidad con privilegios de mayor grado.
- La compartición de recursos también puede aumentar el riesgo de interrupciones de sistemas con fines maliciosos, o involuntarias, y que pueden afectar adversamente a la prestación de servicios. Por ejemplo, la sobrecarga de recursos físicos puede degradar la calidad de funcionamiento de las redes virtuales, con la consiguiente interrupción de la comunicación.

Seguridad de la computación en la nube

En las soluciones de computación la nube, la prestación de servicios y recursos de TI, incluidas las funciones y responsabilidades de seguridad conexas, se subcontrata a un proveedor de servicios en la nube. De un lado, ello permite implantar rápidamente nuevas tecnologías y aumentar la seguridad, puesto que dicho proveedor, sobre la base de las economías de escala, puede ofrecer medidas de protección y control avanzados. Sin embargo, las vulnerabilidades que existen en la nube pueden atraer a los ciberatacantes, puesto que un solo ataque que tenga éxito podría poner en riesgo la seguridad de muchos clientes. Las soluciones de computación en la nube comprenden varias capas de abstracción (de aplicación, sistema operativo, arquitectura y red), de ahí que puedan ser objeto de ataques por medio de varios vectores:

- Las vulnerabilidades en materia de programas informáticos pueden explotarse mediante lenguajes de consulta estructurados, u otros tipos de ataques. A tal efecto, conviene que los clientes de los servicios de computación en la nube sepan quién está a cargo de la implantación de soluciones informáticas (el proveedor de soluciones en la nube, en el caso de las soluciones de *software* como servicio, y el cliente en el caso de las soluciones de infraestructura como servicio y de plataforma como servicio).
- Los proveedores de soluciones de computación en la nube ofrecen una amplia gama de servicios e interfaces de programación de aplicaciones conectadas a Internet para que los clientes puedan administrar y supervisar sus activos. Esa conectividad hace que las soluciones en la nube constituyan un objetivo potencial para los ataques de red, en particular, el rastreo o espionaje del tráfico de red, los ataques DoS y los ataques mediante intermediarios.
- Si un atacante adquiere ilegítimamente datos de acceso de los usuarios, podría acceder asimismo a la interfaz de gestión utilizada por los administradores para gestionar un gran número de activos. En consecuencia, deben establecerse robustos mecanismos de autenticación y autorización, en particular para los empleados con altos privilegios.

[118] Organismo de la Unión Europea para la Ciberseguridad (ENISA), Security aspects of virtualization, 10 de febrero de 2017.

- La multidivisión aumenta el riesgo de filtración o fuga de datos si los controles de división fallan o son objeto de ataques informáticos (fallos de aislamiento).
- Al comenzar a utilizar soluciones de computación en la nube, los clientes suelen tener menos visibilidad y control de sus datos y activos. Ello aumenta el riesgo de supresión segura de los datos almacenados en diversos dispositivos de la infraestructura del proveedor de dichas soluciones de computación en la nube. Conviene verificar que los datos se suprimen de forma segura e íntegra. Este problema se ve agravado con las soluciones que abarcan varias redes de computación en la nube.
- El bloqueo impuesto por proveedores, en virtud del cual se dificulta a los clientes la migración a otro proveedor de soluciones de computación en la nube, puede plantear graves riesgos de seguridad. Los usuarios deben tener en cuenta planes de cambio de proveedor en sus estrategias empresariales y almacenar todos sus datos en un formato normalizado fácilmente transferible.
- Según la Autoridad Reguladora de las Comunicaciones de Namibia, el almacenamiento de datos de clientes en bancos de datos de servicios de computación en la nube situados en otros países es un problema acuciante. En los países en los que se alojan los servidores de datos, los organismos de reglamentación carecen de jurisdicción y no pueden velar por el cumplimiento de la normativa sobre protección de los clientes y la ciberseguridad en el caso de que se produzcan ciberataques susceptibles de provocar el robo de identidades personales, filtración de información personal y, en determinados casos, pérdida de ingresos. Por otro lado, la legislación de dichos países en los que se almacenan los datos podría diferir en materia de acceso a la información y protección de datos, así como adopción de medidas jurídicas para evitar que se produzca un acceso no autorizado a datos personales de los clientes.[119]

Internet de las cosas

Habida cuenta de que el diseño basado en la seguridad se encuentra aún en sus albores, el aumento de la conectividad constituye uno de los principales factores de riesgo actualmente, y plantea graves retos de seguridad:[120]

- Los objetos inteligentes, en particular, cámaras, puertas, dispositivos de refrigeración, sistemas de aire acondicionado y dispositivos portátiles, recaban una gran cantidad de datos (incluidos metadatos). Los atacantes pueden obtener mucha información sobre la vida de sus objetivos al acceder sin autorización a los datos obtenidos a través de los objetos inteligentes del objetivo de que se trate.
- Una amenaza incipiente cada vez más grave en el marco de la IoT es la extorsión por medios informáticos. Los dispositivos inteligentes resultan de gran interés para potenciales atacantes, no solo por la gran cantidad de objetivos que pueden atacar, y la facilidad con la que pueden hacerlo, sino también porque este tipo de ataques puede interrumpir el funcionamiento de los dispositivos y alterar su funcionamiento, y en consecuencia, obligar al pago de un "rescate".[121]
- Los dispositivos de IoT son particularmente vulnerables frente a ataques DoS y DDoS, puesto que la mayoría de ellos poseen capacidades técnicas limitadas (en particular, en cuanto a memoria, almacenamiento y unidad central de procesamiento). La capacidad técnica de los atacantes puede ser muy superior a la de los dispositivos atacados, y en consecuencia, provocar interrupciones de servicio.

---

119 Documento SG2RGQ/75 de la CE 2 del UIT-D de Namibia.
120 Amit Ashbel, The rise of IoT and the associated security risks, 7 de julio de 2016.
121 Syed Rameem Zahra y Mohammad Ahsan Chishti, RansomWare and Internet of Things: A New Security Nightmare, *Proceeding of the 9th International Conference on Cloud Computing, Data Science Engineering (Confluence)*, Uttar Pradesh, India, 10-11 de enero de 2019.

- La limitación de recursos de los dispositivos IoT es un reto fundamental al incorporar medidas de seguridad que podrían requerir una capacidad de cálculo elevada.[122]
- La complejidad de la IoT constituye un aspecto clave en materia de seguridad. Los dispositivos combinan varias tecnologías, en particular, la virtualización, la computación en la nube, los sensores y las redes, que conllevan sus propias vulnerabilidades. La seguridad de la IoT conlleva asimismo la seguridad de todos esos componentes. Análogamente, las aplicaciones de IoT abarcan varias esferas (automatización del hogar, asistencia sanitaria, dispositivos portátiles, etc.), con necesidades y riesgos de seguridad de índole diversa.
- Pese a que los ataques basados en Internet son los más habituales, los dispositivos de IoT también pueden ser objeto de ataques físicos. En zonas con poca o ninguna vigilancia, los atacantes pueden acceder fácilmente a los dispositivos IoT y manipularlos.
- Los dispositivos IoT también pueden utilizarse como vectores para lanzar ataques DDoS. En 2016, por ejemplo, un famoso proveedor de sistemas de nombres de dominio fue víctima de un ataque DDoS que tuvo su origen en decenas de millones de direcciones IP, y la mayor parte del tráfico malicioso procedía de dispositivos IoT como impresoras, encaminadores y cámaras.[123]

Tecnologías 5G

La quinta generación de tecnología de redes de comunicaciones, o 5G, ofrecerá una conexión más eficaz y de mejor calidad de alta velocidad y baja latencia, a fin de lograr la máxima calidad de funcionamiento posible de aplicaciones tecnológicas incipientes en esferas como la energía, la sanidad y el sector de la producción industrial. Esos activos son de interés para los atacantes, y su vulnerabilidad intrínseca dificulta en gran medida la ciberseguridad. Por otro lado, puesto que las soluciones 5G aún se encuentra en una fase piloto, no se dispone de información y datos suficientes sobre incidentes de ciberataques, lo que dificulta aún más la evaluación de los posibles riesgos:[124]

- El panorama de los riesgos asociados a las tecnologías 5G es muy amplio y heterogéneo; al utilizar diversas tecnologías, las vulnerabilidades y los riesgos que cabe considerar también son muy diversos. En particular, las redes y activos 5G pueden ser objeto de ataques como consecuencia de las lagunas de seguridad de las tecnologías de segunda, tercera y cuarta generación, las deficiencias habituales basadas en IP y los flujos asociados a la tecnología de virtualización. Los atacantes también pueden hacer hincapié en activos específicos de las tecnologías 5G, como elementos de la red troncal, puntos de acceso y elementos periféricos.
- Los ataques contra las redes 5G pueden incluir intentos de robo, manipulación o destrucción de datos, interceptación o alteración de comunicaciones, daño a activos físicos, o interrupción del suministro de servicios. Las redes 5G facilitarán la conexión de un amplio conjunto de sectores e industrias verticales, lo que muy probablemente modificará el panorama de la ciberseguridad y dará lugar a nuevas vulnerabilidades.
- Un factor de amenaza crítico viene asociado a las cadenas de suministro, en particular las de proveedores de servicios y vendedores. El riesgo consiste en que un proveedor pueda incorporar maliciosamente en sus productos "puertas traseras" ocultas o programas informáticos, y provocar fallos críticos. La implantación de actualizaciones automáticas (e incontroladas) y la alteración de funciones también plantean riesgos de seguridad. La relación entre las tecnologías 5G y la seguridad nacional es manifiesta, y los proveedores deben escogerse meticulosamente sobre la base de un enfoque orientado al riesgo.

---

122 Ammar Rayes y Samer Salam, Internet of Things From Hype to Reality: The Road to Digitization, Springer International Publishing, 2019.

123 Nicole Perlroth, Hackers Used New Weapons to Disrupt Major Websites Across U.S., *The New York Times*, 21 de octubre de 2016.

124 ENISA, ENISA threat landscape for 5G Networks, noviembre de 2019.

Inteligencia artificial

La utilización generalizada de soluciones de inteligencia artificial en varios sectores de la sociedad repercutirá en el panorama de ciberseguridad de varias maneras. Dichos activos pueden ser objeto de ataque de actores maliciosos, o utilizados por adversarios y defensores:

- Los activos de IA pueden manipularse mediante la modificación de decisiones y comportamientos automatizados, en particular la alteración de datos y de modelos de categorización, y las "puertas traseras".[125] Todos esos métodos aprovechan la capacidad de aprendizaje del sistema para influir de forma adversa en el resultado, al proporcionar a dicho sistema datos e información erróneos.[126]
- Los piratas informáticos recurren a soluciones de IA para aumentar su eficacia y capacidad. La IA puede utilizarse para desarrollar programas maliciosos que permitan superar las medidas defensivas de forma autónoma, adaptar su estrategia en función de los resultados satisfactorios y mejorar constantemente su funcionamiento.
- La IA también constituye un recurso de protección muy útil. Puede aumentar sustancialmente la resistencia de un sistema al mejorar las actividades defensivas habituales, en particular la detección de amenazas y anomalías, las medidas de respuesta frente a incidentes y el análisis de amenazas.

5.2.2 Riesgos con respecto a la Industria 4.0

En el marco de la Industria 4.0 se llevan a cabo actividades de automatización, IoT, virtualización, analítica e IA con respecto a varios sectores verticales. Esas tecnologías permiten recopilar, almacenar, compartir e interpretar enormes cantidades de datos, y pueden aportar mejoras sustanciales en términos de velocidad, eficacia, rentabilidad y suministro de servicios. La Industria 4.0 abarca diversos sectores, cada uno de los cuales es susceptible de amenazas y riesgos de seguridad específicos.

Hogares inteligentes

Los hogares inteligentes son uno de los sectores verticales que abarca la Industria 4.0, en particular con respecto al consumo inteligente de energía y sistemas de iluminación o calefacción. Los hogares inteligentes contienen una gran variedad de objetos inteligentes que utilizan sensores y activadores y se gestionan a distancia a través de Internet.[127] La conexión de dispositivos a Internet conlleva varios riesgos de seguridad:

- Los hogares inteligentes generan grandes cantidades de datos que son vulnerables frente a ataques. Como señaló el Ministerio de Correos y Nuevas Tecnologías de la Información y la Comunicación de Chad, los objetos conectados (incluidas las televisiones inteligentes) están expuestos a amenazas de seguridad de sistemas de información. Por ejemplo, la utilización de televisiones conectadas puede facilitar el acceso de personas no autorizadas a información personal a través de Internet, o el robo de identidades. Los objetos conectados son vulnerables en la misma medida que los ordenadores personales conectados a Internet, y están expuestos asimismo a programas maliciosos.[128]

---

125 Battista Biggio y Fabio Roli, Wild patterns: Ten years after the rise of adversarial machine learning, *Pattern Recognition* vol. 84, diciembre de 2018, pp. 317-31.

126 Matthew Jagielski *et al.*, Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning, *IEEE Symposium on Security and Privacy (SP)*, 2018.

127 Ado Adamou Abba Ari *et al.*, Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges, *Applied Computing and Informatics*, 31 de julio de 2020.

128 Documento 2/140 de la CE 2 del UIT-D de Chad.

- Los dispositivos inteligentes incorporan pocas medidas de seguridad y pueden ser objeto de ataques de piratas informáticos de forma muy sencilla. Los atacantes que obtienen el control de dichos dispositivos pueden acceder prácticamente a toda la red doméstica y tomar el control de otros nodos.
- Por lo general, los dispositivos inteligentes cuentan con escasos recursos informáticos, de ahí que sean especialmente vulnerables frente a ataques DoS y DDoS, que hacen que dichos dispositivos, o su red, no estén disponibles temporalmente para los usuarios previstos.

Ciudades inteligentes

Las ciudades inteligentes conjugan la utilización de tecnologías incipientes con la integración de datos y la automatización de tareas, a fin de optimizar la organización de las ciudades y ofrecer mejores servicios. Las ciudades inteligentes se basan en amplios flujos de datos compartidos entre servicios críticos, en particular en los sectores del transporte, el suministro de energía y la asistencia sanitaria, que están cada vez más interconectados. La cantidad de datos generados y la función de los mismos con respecto al funcionamiento de las ciudades inteligentes da lugar a la acuciante necesidad de ciberseguridad para proteger la privacidad de la información y la integridad de los activos digitales frente a amenazas de seguridad de índole diversa:

- ***Cibersanidad***: la mayor dependencia de la tecnología y el aumento de la cantidad de datos sanitarios hacen que los proveedores de servicios sanitarios tengan que proteger la información sensible y garantizar la prestación de servicios. Pese a que aún no consta ningún incidente específico, en diversos simulacros se ha demostrado que es posible desconectar de forma inalámbrica desfibriladores cardíacos implantables[129], acceder ilegítimamente a bombas de insulina para liberar dosis letales[130] o acceder a los sistemas de supervisión de pacientes para modificar sus constantes vitales en tiempo real.[131]
- ***Redes inteligentes***: se trata de un componente clave de las ciudades inteligentes. Utilizan dispositivos bidireccionales, en particular, sensores, activadores y contadores, que permiten mantener un equilibrio y una supervisión de forma ininterrumpida de los flujos de energía que abarcan productores y consumidores.[132] Habida cuenta de que las redes inteligentes se basan en protocolos de TIC y en conexiones a Internet, son vulnerables a los ciberataques.[133] Las redes inteligentes son un objetivo de gran interés para los atacantes; sin embargo, debido a su compleja arquitectura, provocar en ellas daños a gran escala requiere recursos técnicos y de planificación muy sofisticados. Hasta ahora solo se tiene constancia de dos casos de interrupción grave de suministro eléctrico como consecuencia de ciberataques, a saber, los ataques BlackEnergy3 y Crashoverride, presumiblemente perpetrados por agentes estatales.[134]
- ***Transporte inteligente***: los activos digitales, los sistemas físicos, las redes de comunicaciones y la automatización pueden incorporarse a las infraestructuras de transporte para optimizar su calidad y eficacia. Al modificar datos e información, los atacantes pueden dificultar el tráfico o provocar incidentes. Por otro lado, los sistemas

[129] Daniel Halperin *et al.*, Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses, *IEEE Symposium on Security and Privacy (SP)*, 2008.
[130] Arundhati Parmar, Hacker shows off vulnerabilities of wireless insulin pumps, *MedCityNews*, 1 de marzo de 2012; David Klonoff, Cybersecurity for Connected Diabetes Devices, *Journal of Diabetes Science and Technology* 9, vol. 9, N° 5, 16 de abril de 2015.
[131] Douglas McKee, 80 to 0 in Under 5 Seconds: Falsifying a Medical Patient's Vitals, McAfee, 11 de agosto de 2018.
[132] Lindah Kotut y Luay A. Wahsheh, Survey of Cyber Security Challenges and Solutions in Smart Grids, *2016 Cybersecurity Symposium* (CYBERSEC).
[133] Muhammed Zekeriya Gunduz y Resul Das, Cyber-security on smart grid: Threats and potential solutions, *Computer Networks*, vol. 169, 14 de marzo de 2020.
[134] Dragos, Inc, CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids, 12 de junio de 2017.

de transporte inteligente requieren un flujo de información personal privada que debe ser objeto de protección.

Internet de las cosas industrial

Internet de las cosas industrial (IIoT) constituye una adaptación de la IoT al sector industrial. La combinación de robótica y automatización puede brindar amplios beneficios a las empresas de dicho sector, en particular, la mejora de la calidad, la rentabilidad y el mantenimiento del proceso de producción. Esos sistemas ciberfísicos poseen características y requisitos específicos que dificultan la implantación de las medidas de ciberseguridad tradicionales.

Los sistemas ciberfísicos son entornos en tiempo real que poseen un elevado grado de determinismo, en los que la disponibilidad de datos reviste más importancia que la integridad y la confidencialidad.[135] En esos sistemas, los componentes digitales interactúan con procesos físicos como el movimiento de objetos, las reacciones químicas, la liberación de sustancias y los procesos de refrigeración, y los flujos de datos constituyen la base de la ejecución de las tareas. A tal efecto, la realización de controles de seguridad habituales, como los programas antivirus, el cifrado o los cortafuegos, podría dificultar el flujo de datos y el desarrollo de actividades, y provocar retrasos que, aunque cuantitativamente no revistan importancia, podrían afectar ampliamente a las operaciones.[136]

Por otro lado, la mayoría de equipos de los sistemas ciberfísicos no pueden aplicar sofisticadas medidas de seguridad ni realizar actualizaciones, de ahí que los objetos conectados a Internet sean particularmente vulnerables. Los ciberataques contra sistemas ciberfísicos industriales pueden provocar graves daños económicos al alterar las operaciones de una planta y, en consecuencia, su nivel de producción.

No obstante, lo que más inquietud provoca es que, al manipular el flujo de datos, los ciberatacantes podrían modificar el funcionamiento de un sistema hasta que este alcance un punto de ruptura mecánica, lo que provocaría un efecto cinético con graves consecuencias para la seguridad pública. Por ejemplo, si un atacante suministra al sistema cifras alteradas que indican al controlador la disminución de un valor determinado de temperatura de forma demasiada rápida, el controlador lo compensará automáticamente aumentando el nivel de temperatura, efecto susceptible de provocar un sobrecalentamiento no detectado.[137] Por ejemplo, en 2014 una planta de producción de acero en Alemania fue objeto de un ataque informático, y los atacantes, al impedir que un horno se apagara adecuadamente, provocaron daños físicos masivos en componentes críticos.[138]

Los ciberataques que provocan efectos físicos en las operaciones son de gran complejidad, y requieren no solo un conocimiento pormenorizado de los activos digitales utilizados, sino del proceso físico que es objeto de ataque, así como una comprensión muy cabal de todas las variables posibles. En consecuencia, los atacantes persistentes avanzados y los intermediarios

---

[135] Roberto Setola et al., Cyber threats for operational technologies, *International Journal of System of Systems Engineering*, vol. 10, N° 2, 2020.
[136] Roberto Setola *et al.*, An overview of Cyber Attack to Industrial Control System, *Chemical Engineering Transactions*, vol. 77, 2019.
[137] Stephen McLaughlin *et al.*, The Cybersecurity Landscape in Industrial Control Systems, *Proceedings of the IEEE*, vol. 104, N° 5, mayo de 2016.
[138] Robert Lee *et al.*, German Steel Mill Cyber Attack, Industrial Control Systems Defense Use Case, 30 de diciembre de 2014.

con patrocinio estatal son los más proclives a disponer de los recursos técnicos y organizativos necesarios para llevar a cabo este tipo de operaciones.

5.3 Soluciones implantadas e incipientes

Una proporción sustancial de dispositivos IoT no incorporan ninguna función básica de ciberseguridad. En octubre de 2018, tras 18 meses de colaboración con representantes del sector y expertos del Centro Nacional de Ciberseguridad, el Departamento de Tecnologías Digitales, Cultura, Medios de Comunicación y Deporte del Reino Unido publicó sus Directrices sobre seguridad de los usuarios de la IoT.[139] Las 13 directrices voluntarias publicadas proporcionan parámetros de referencia sobre dispositivos de IoT que los fabricantes deben tener en cuenta en sus productos para garantizar un "diseño seguro". Las citadas directrices contribuyeron a la elaboración de la norma ETSI TS 103 645 sobre seguridad de IoT, la primera de aplicación mundial.[140]

Algérie Télécom también ha subrayado la importancia de elaborar guías y recomendaciones sobre la seguridad de tecnologías incipientes como la computación en la nube e IoT, que se prevé que pasen a constituir el elemento fundamental del desarrollo de los sistemas de información y de la economía digital.[141]

En los **Cuadros 1** y **2** siguientes se enumeran respectivamente las Recomendaciones del UIT-T pertinentes a los efectos de protección de los sistemas de computación en la nube y de sistemas de IoT, en términos de infraestructuras, aplicaciones, datos y privacidad.

Cuadro 1 – Arquitectura de seguridad para la protección de infraestructuras, aplicaciones, datos y la privacidad en los sistemas de computación en la nube

Título	Tema	Institución	Enlace
Visión general de la seguridad de la computación en la nube			
UIT-T X.1601	Marco de seguridad para la computación en la nube	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12613
Diseño de seguridad de la computación en nube			
UIT-T X.1602	Requisitos de seguridad para el entorno de aplicación Software como servicio	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12615
UIT-T X.1603	Requisitos de seguridad de los datos para el servicio de control de la computación en la nube	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13406
UIT-T X.1604	Requisitos de seguridad de la red como servicio (NaaS) en la computación en la nube	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14093

[139] Reino Unido, Departamento de Tecnologías Digitales, Cultura, Medios de Comunicación y Deporte, Code of Practice for Consumer IoT Security, octubre de 2018.
[140] ETSI, ETSI TS 103 645 V1.1.1 (2019-02); Cyber Security for Consumer Internet of Things.
[141] Documento 2/66 de la CE 2 del UIT-D de Algérie Télécom SPA (Argelia).

Cuadro 1 – Arquitectura de seguridad para la protección de infraestructuras, aplicaciones, datos y la privacidad en los sistemas de computación en la nube (continuación)

Título	Tema	Institución	Enlace
UIT-T X.1605	Requisitos de seguridad de la infraestructura pública como servicio (IaaS) en la computación en la nube	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14094
UIT-T X.1631	Tecnología de la información – Técnicas de seguridad – Directrices basadas en la norma ISO/IEC 27002 para la gestión de la seguridad de la información en sistemas de computación en la nube	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12490
Prácticas idóneas y directrices en materia de seguridad de la computación en la nube			
UIT-T X.1641	Directrices para la seguridad de los datos de clientes de los servicios en la nube	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12853
UIT-T X.1642	Directrices para la seguridad operativa de la computación en la nube	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12616

Cuadro 2 – Arquitectura de seguridad para la protección de infraestructuras, aplicaciones, datos y la privacidad en los sistemas de IoT

Título	Tema	Institución	Enlace
Seguridad en la Internet de las cosas (IoT)			
UIT-T X.1361	Marco de seguridad para la Internet de las cosas basado en el modelo de pasarela	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13607
UIT-T X.1362	Procedimiento de encriptación simple para la Internet de las cosas (IoT)	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13196
UIT-T X.1364	Requisitos y marco de seguridad de la Internet de las cosas de banda estrecha	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14088
UIT-T X.1365	Metodología de seguridad para el uso de criptografía basada en la identidad para dar soporte a servicios de Internet de las cosas mediante redes de telecomunicaciones	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14089
UIT-T X Sup.31	UIT-T X.660 – Suplemento sobre directrices para la utilización de identificadores de objeto en Internet de las cosas	UIT	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13411

Técnicas y marcos de seguridad incipientes suplementarios

- Las aplicaciones de IA, en particular el aprendizaje automático y el aprendizaje en profundidad, pueden respaldar notablemente las estrategias de ciberseguridad en términos de eficiencia y rentabilidad. Las soluciones utilizadas se basan en técnicas de regresión, clasificación y agrupación con objeto de detectar anomalías, identificar tipologías de ataques y formular posibles medidas de respuesta y reparación. Los sistemas de inteligencia artificial también pueden mejorar las actividades de respuesta frente a incidentes al proponer acciones específicas frente a determinados incidentes. También pueden mejorar las actividades de gestión de riesgos al asignar automáticamente valores de riesgo a nuevas vulnerabilidades y configuraciones erróneas con arreglo a su descripción y prevenir ataques de forma proactiva al facilitar en gran medida la obtención, el tratamiento y la utilización de datos sobre amenazas, actores, ataques, programas maliciosos, vulnerabilidades e indicadores de riesgo.[142]
- Las características específicas de la tecnología de libro mayor distribuido (DLT) también pueden mejorar las aplicaciones de seguridad.[143] En primer lugar, el almacenamiento basado en DLT está descentralizado, lo que reduce sustancialmente el riesgo de que se produzcan fugas de datos, puesto que los atacantes no pueden acceder a todos los datos almacenados a través de un único punto de acceso. Análogamente, la descentralización brinda ventajas de seguridad esenciales a las redes IoT, organizadas habitualmente con respecto a la lógica del modelo cliente-servidor, en virtud del cual una autoridad central gestiona los datos y los dispositivos de la red. Las aplicaciones DLT permiten a los dispositivos de IoT detectar anomalías y aislar los nodos cuyo funcionamiento sea inusual. Por otro lado, la DLT puede fomentar la confianza en las redes de IoT, al garantizar la disponibilidad, auditoría, responsabilidad, integridad y confidencialidad de los datos intercambiados.[144]
- El método de gestión, automatización y respuesta en materia de seguridad (SOAR) abarca soluciones que permiten conectar herramientas y sistemas de seguridad para llevar a cabo actividades como la gestión de vulnerabilidades, la adopción de medidas de respuesta frente a incidentes y la automatización de operaciones de seguridad de forma integrada y orgánica. La automatización de los procesos de seguridad permite al sistema aplicar medidas de reparación y llevar a cabo actividades de mantenimiento (análisis de vulnerabilidades y control de accesos y registros) sin intervención humana.
- Otra posibilidad se basa en los modelos de confianza cero, en virtud de los cuales los entornos de red se segmentan de forma interna y los accesos se administran según el principio de menor privilegio posible. Ello conlleva que cada módulo, incluidos los usuarios, los dispositivos, las interfaces de programación de aplicaciones y los dispositivos IoT, únicamente puedan acceder a los recursos, datos y activos necesarios para desempeñar su función de forma legítima. Los modelos de confianza cero aumentan en gran medida la seguridad interna, puesto que el desplazamiento lateral y la jerarquía de privilegios dificultan la labor de los atacantes que, para obtener acceso a toda la red, tendrían que fijar varios dispositivos como objetivo.
- Los intermediarios de seguridad de acceso a los sistemas de computación en la nube constituyen nodos de aplicación de políticas entre los usuarios y los proveedores de dichos sistemas de computación. Por ejemplo, las políticas de seguridad pueden abarcar las actividades de autenticación, inicio de sesión único, autorización, asignación de datos de acceso, establecimiento de perfiles de dispositivos, cifrado, utilización de testigos, registro, emisión de alertas y detección/prevención de programas maliciosos.[145]

---

142 Padmavathi Ganapathi y D. Shanmugapriya, Handbook of Research on Machine and Deep Learning Applications for Cyber Security, *IGI Global*, 2019; y Dave Shackleford, Who's Using Cyberthreat Intelligence and How?, *SANS*, 12 de febrero de 2015.

143 Nir Kshetri, Blockchain's roles in strengthening cybersecurity and protecting privacy, *Telecommunications Policy*, vol. 41, Nº 10, noviembre de 2017.

144 Ben Cole, The 'supply chain of trust' inherent to IoT data security, *IoT Agenda*, 28 de noviembre de 2016.

145 Gartner, Cloud Access Security Brokers (CASBs).

- La gestión de accesos con privilegios se refiere al conjunto de herramientas y soluciones que permite supervisar y proteger las cuentas mediante establecimiento de privilegios, en particular, las cuentas de administrador utilizadas para acceder a activos, datos y recursos críticos. Esas soluciones protegen las cuentas críticas mediante un repositorio seguro y supervisado, a fin de reducir el riesgo de robo de datos de acceso.
- Conviene que las organizaciones pasen de un enfoque de desarrollo y operaciones (DevOps) a otro de desarrollo, seguridad y operaciones (DevSecOps), que incorpore la seguridad al desarrollo y a las operaciones de forma intrínseca. Con arreglo a los marcos y las herramientas DevSecOps, en lugar de asociarse a productos finales (como programas informáticos y aplicaciones), la seguridad se considera una característica integral y esencial desde la primera fase de desarrollo. Ese enfoque aumenta la seguridad, mitiga los riesgos y reduce los costos en materia de conformidad.
- En virtud del Marco de Gartner para la evaluación adaptativa ininterrumpida de riesgos y confianza (CARTA), se propone un enfoque adaptativo con respecto a la seguridad que permite fundamentar las decisiones en el riesgo y la eficacia.[146] El marco CARTA comprende tres fases: "ejecutar", que se centra en el análisis de las principales amenazas; "construir", referente a las amenazas y vulnerabilidades identificadas durante el desarrollo de productos y operaciones; y "planificar", que permite aplicar la analítica para determinar los riesgos de seguridad y evaluar si su mitigación puede repercutir adversamente en la productividad.[147]

Soluciones rentables

- Según el Departamento de Tecnologías Digitales, Cultura, Medios de Comunicación y Deporte del Reino Unido, al hacer hincapié en mermar el rendimiento de la inversión en ataques poco sofisticados y muy habituales pueden comenzarse a mitigar los efectos de los ciberataques a escala y obtener amplios beneficios a escala mundial. El método de Ciberdefensa Activa tiene por objeto elevar el costo y el riesgo de organizar ciberataques básicos contra el Reino Unido, con la consecuente disminución del rendimiento de la inversión para los delincuentes.[148] En 2018, dicho método arrojó los mejores resultados a través de su servicio de petición de baja, en virtud del cual se identifican sitios maliciosos (ya sea mediante ataques o infraestructura de apoyo a esos ataques) y se notifica a su proveedor de alojamiento o a su propietario que deben ser dados de baja en Internet; mediante este método se suprimieron 192 256 sitios web fraudulentos, el 64 por ciento de los cuales se dieron de baja en un plazo de 24 horas. Por otro lado, se suprimieron 22 133 campañas de usurpación de identidad con dirección IP registrada en el Reino Unido (que provocaron 142 203 ataques en total), y se dieron de baja 14 124 sitios de usurpación de identidad gubernamental.[149]
- Según la empresa NRD Cyber Security, de Lituania, con objeto de lograr un resultado satisfactorio en materia de seguridad del entorno digital a escala nacional, los EIISI nacionales y sectoriales deben desempeñar las funciones de puntos de contacto, coordinadores de las medidas de respuesta frente a incidentes y analistas, y facilitar el desarrollo de capacidades suplementarias autónomas en materia de ciberseguridad en el marco de empresas, comunidades de profesionales, centros educativos, instituciones de investigación, eventos, reuniones, conferencias y EIISI privados e internos.[150]
- Por otro lado, la empresa Guardtime, de Estonia, considera que los ciberejercicios son esenciales para fomentar una ciberresiliencia sostenible, puesto que ayudan a los equipos a comprender los procesos necesarios para superar las cibercrisis. Estonia recomienda desarrollar un programa de gobernanza de la ciberresiliencia que abarque la educación,

---

146 Gartner, The Gartner IT Security Approach for the Digital Age, 12 de junio de 2017.
147 Gartner, Gartner Keynote: Leverage Automation for Modern Security, 17 de junio de 2019.
148 Ian Levy y Maddy S., Active Cyber Defence – The Second Year, Centro Nacional de Ciberseguridad del Reino Unido, 15 de julio de 2019.
149 Documento SG2RGQ/175 de la CE 2 del UIT-D del Reino Unido.
150 Documento 2/172 de la CE 2 del UIT-D de NRD Cyber Security (Lituania).

la formación y los ciberejercicios, e incluya eventos localizados y ejercicios periódicos personalizados a escala nacional. Dichos programas deben tener en cuenta diversos aspectos relativos a la estructura orgánica nacional y a la situación socioeconómica, las funciones y responsabilidades de las partes interesadas, el entorno normativo nacional, las asociaciones de cada país a escalas regional e internacional, y los riesgos que afronta el país como consecuencia de la evolución de las ciberamenazas.[151]

[151] Documento SG2RGQ/32 de la CE 2 del UIT-D de Guardtime AS (Estonia).

Capítulo 6 – Contribución de la ciberseguridad a la protección de la información personal

6.1 Introducción

El desarrollo de nuevas tecnologías de la información ha propiciado el surgimiento de nuevos servicios que cada vez son más útiles para uso cotidiano. No obstante, esas tecnologías de la información también modifican de forma bilateral los riesgos para la privacidad y la protección de datos que deben afrontar las personas. Pese a que siguen surgiendo nuevos riesgos en materia de datos personales, cabe utilizar técnicas de índole diversa para mitigar o evitar dichos riesgos. De ahí que sea necesario hacer hincapié en la ciberseguridad y en las tecnologías que permiten mejorar la privacidad y la protección de datos personales, en particular, las técnicas de pseudonimización y el diseño basado en la privacidad.

La pseudonimización es un procedimiento de gestión y desidentificación de datos mediante el cual los campos de información de identificación personal de un registro de datos se sustituyen por un identificador artificial, o "seudónimo", o varios. Un único seudónimo para cada campo sustituido, o conjunto de campos sustituidos, dificulta la identificación del registro de datos, sin que deje de ser adecuado a los efectos de análisis y procesamiento de datos.[152] La pseudonimización puede contribuir a proteger la información de identificación personal y reducir la carga de las entidades que obtienen y almacenan dichos datos.

En relación con la privacidad basada en el diseño, no es necesario esperar hasta que se produzca una fuga de datos para tomar medidas de seguridad. En su lugar, los desarrolladores prevén o anticipan las amenazas de privacidad o las evitan mediante medidas preventivas, en particular actividades de planificación o diseño de servicios.[153] La diferencia entre ambos enfoques reside en que, si bien la pseudonimización requiere ciertas medidas de índole técnica, el diseño basado en la privacidad ofrece a los responsables del tratamiento de datos la flexibilidad necesaria para establecer qué medidas técnicas suplementarias cabe adoptar para mejorar la seguridad y la privacidad de los datos.

6.2 Panorama jurídico y prácticas idóneas en los Estados Miembros

En la Ley General de Protección de Datos de Brasil, recientemente aprobada, se proporciona la definición de los distintos tipos de datos personales, y se establecen los permisos jurídicos a los efectos de su procesamiento a escalas nacional e internacional, los derechos fundamentales de los interesados y la constitución de una autoridad nacional de protección de datos.[154] En

[152] Wikipedia. https://en.wikipedia.org/wiki/Pseudonymization.
[153] El diseño basado en la privacidad se utilizaba en el marco de la arquitectura aplicada, si bien ese concepto era secundario. Comenzó a revestir importancia después de que la Dra. Ann Cavoukian, Comisionada de Información y Privacidad de datos de Ontario (Canadá), se refiriera al mismo a mediados del decenio de 1990.
[154] Documento SG2RGQ/143 de la CE 2 del UIT-D de Brasil.

el marco de dicha ley se establecen los principios de minimización de los datos, prevención de fuga de información y seguridad de los datos, y se estipulan normas específicas por las que se rigen esas áreas. La ley también abarca el diseño basado en la seguridad, y prevé que las medidas de seguridad para proteger los datos personales se apliquen desde la etapa de concepción del producto o servicio hasta su implantación.

En 2017, China publicó de forma oficial un conjunto de normas nacionales sobre especificaciones de seguridad de la información personal en relación con la tecnología de la seguridad de la información, que complementan los requisitos de seguridad de la información personal establecidos en su Ley de Ciberseguridad. Dichas normas proporcionan directrices e instrucciones operacionales. China prosigue su labor de estudio y formulación de normas sobre protección de la información personal.[155]

En China, las empresas locales de seguridad de datos también estudian y desarrollan de forma activa productos y servicios de seguridad, en particular en las esferas de la prevención de la pérdida de datos, la auditoría de seguridad de las bases de datos, la supervisión de fugas en las bases de datos, el cifrado de las bases de datos y el enmascaramiento de datos, con miras a proporcionar apoyo técnico para la protección de la información personal.

La República de Corea ha introducido una importante enmienda a su Ley de Protección de la Información Personal con objeto de proporcionar medidas técnicas de protección de los datos personales.[156] Dicha enmienda incorporó cambios para racionalizar la supervisión reglamentaria e introducir el concepto de "datos pseudonimizados", que permite un control y procesamiento de datos de forma más segura, al tiempo que mitiga el riesgo de utilización indebida y fuga de datos mediante otras medidas tecnológicas y orgánicas, en particular la protección de datos en la fase de diseño y por defecto.

Por otro lado, el Gobierno de la República de Corea ha publicado varias directrices en materia de protección relativas al tratamiento automático de datos personales. Pese a que las nuevas tecnologías, en particular el análisis de macrodatos mediante IA y la utilización de sensores en dispositivos de IoT para obtener datos, facilitan la prestación de servicios innovadores, existen dificultades para comprender el flujo del tratamiento de datos personales y adoptar medidas de respuesta de seguimiento. Con respecto al tratamiento automático de los datos personales de dispositivos de IoT, las directrices fomentan la privacidad desde la etapa de diseño, en la que se tiene muy en cuenta la posibilidad de que se produzcan fugas de datos personales en las primeras etapas de planificación y a lo largo de la vida útil de los datos.

A continuación se enumeran las diez normas de protección para el procesamiento automatizado de datos personales que figuran en las directrices:

- Fase de planificación
  - Norma 1: Confirmación de los datos personales necesarios para los servicios
  - Norma 2: Confirmación de la observancia de los aspectos jurídicos al obtener datos personales
- Fase de diseño

[155] Documento 2/156 de la CE 2 del UIT-D de China.
[156] Documento 2/342 de la CE 2 del UIT-D de la República de Corea.

- Norma 3: Minimización de datos y procesamiento únicamente de la información personal necesaria
- Norma 4: Aplicación de medidas de seguridad adecuadas en cada fase del procesamiento de datos personales
- Norma 5: Difusión transparente de los procedimientos y métodos de procesamiento de datos personales
- Norma 6: Garantizar que los interesados puedan ejercer fácilmente sus derechos
- Norma 7: Instrucciones claras para los interesados al proporcionar y encargar datos personales a terceros
- Norma 8: Supresión de los datos personales, al tiempo que se impide la obtención de más datos después de que el interesado rescinda el servicio
- Norma 9: Formulación de planes que permitan garantizar el derecho de los interesados después de la prestación del servicio

– Fase de examen

- Norma 10: Examen de los factores de riesgo relacionados con la fuga de datos personales antes de la prestación del servicio.

A raíz de la reciente necesidad de rastrear los casos confirmados de COVID-19 en todo el mundo, la República de Corea ha adoptado diversas medidas institucionales y técnicas para proteger los datos personales. Además de garantizar la base jurídica para el seguimiento de los pacientes confirmados mediante la revisión de la normativa pertinente, se han adoptado medidas de índole técnica para clasificar y gestionar la información de identificación con el fin de evitar posibles fugas de datos personales. Los datos clasificados se utilizan para realizar estudios epidemiológicos solo si se producen casos confirmados, y la información personal de usuarios y visitantes se gestiona de forma segura, por ejemplo, al destruirse automáticamente cuatro semanas después de su generación.[157]

Una empresa italiana ha desarrollado una metodología propia que pueden utilizar fácilmente las organizaciones para elaborar una lista de actividades técnicas y facilitar la conformidad de la infraestructura de computación en la nube (privada, pública o híbrida) en materia de privacidad[158]. Dicha metodología incluye una propuesta para definir las directrices generales que podrían aplicar los Estados Miembros para poner en marcha sus propios configuradores a escala nacional con el fin de normalizar el cumplimiento en varios países de manera más eficaz y rentable, al utilizar los sistemas de computación en la nube como sólidas plataformas para promover la economía digital.

En virtud del Artículo 25 del Reglamento General de Protección de Datos (RGPD) de la Unión Europea sobre protección de datos desde la etapa de diseño y por defecto, que constituye un nuevo caso de prácticas idóneas, se considera la privacidad desde el diseño el método más adecuado para mitigar los riesgos asociados a la protección de datos personales que plantean los dispositivos de IoT, los macrodatos y la IA, entre otras nuevas tecnologías. Con arreglo al concepto de diseño basado en la privacidad, las medidas técnicas y de organización adecuadas para garantizar la seguridad y la privacidad de los datos personales se integran en el todo el ciclo de vida útil de los productos, los servicios, las aplicaciones y los procedimientos

[157] Documento SG2RGQ/268 de la CE 2 del UIT-D de la República de Corea.
[158] Documento SG2RGQ/25 de la CE 2 del UIT-D de Proge-software (Italia).

empresariales y técnicos de una organización determinada. Las medidas técnicas pueden incluir, entre otras, la pseudonimización y la minimización de datos.[159]

El Organismo de la Unión Europea para la Ciberseguridad (ENISA) ha presentado ocho estrategias clave para ayudar a las empresas a fomentar el diseño basado en la privacidad con objeto de examinar enfoques, estrategias y factores técnicos que faciliten la protección de datos personales.[160]

Cuadro 3 – Ocho estrategias clave para fomentar el diseño basado en la privacidad

	Principio	Contenido
1	Minimizar	Reducir todo lo posible la cantidad de datos personales procesados, y hacerlo de forma clara para garantizar en la medida de lo posible la privacidad.
2	Ocultar	Ocultar la transmisión de texto sin cifrar al procesar datos personales a fin de evitar su acceso desde el exterior.
3	Clasificar	Clasificar y almacenar diversos datos personales para evitar la discriminación de personas específicas en la base de datos.
4	Agregar	Agregar grandes cantidades de datos personales procesados a fin de reducir todo lo posible la discriminación de personas y clasificar los resultados del procesado de datos para impedir toda discriminación.
5	Informar	Informar a los interesados del proceso íntegro de procesamiento de datos personales para proporcionar una comprensión cabal de los fines a los que se destinan los datos.
6	Controlar	Controlar la utilización de datos personales. Los interesados deben comprender íntegramente el procesamiento de datos personales y estar en medida de ejercer sus derechos en relación con la utilización indebida de sus datos o la inobservancia de los niveles de seguridad establecidos con arreglo a la quinta estrategia, "Informar", anteriormente enumerada.
7	Aplicar las normativas	La política interna de protección de datos personales debe estar en consonancia con las normativas y disposiciones jurídicas que cabe aplicar.
8	Demostrar	Demostrar el cumplimiento de las disposiciones jurídicas pertinentes, en particular, la implantación eficaz de políticas de protección de datos personales y la adopción de medidas con carácter inmediato frente a incidentes que conlleven la fuga de datos.

Por otro lado, ENISA ha formulado varias propuestas sobre actividades de protección de la privacidad y de los datos que deben llevar a cabo las partes interesadas. Recomienda que los responsables políticos promuevan y respalden el establecimiento de nuevos incentivos para fomentar los servicios de protección de datos personales, y que los grupos de estudios y

[159] Unión Europea, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de personas físicas con respecto al procesamiento y a la transmisión de datos personales, en virtud del cual se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
[160] ENISA, Privacy and Data Protection by Design – from policy to engineering, diciembre de 2014.

desarrollo analicen métodos de ingeniería para proteger los datos personales por medio de un enfoque interdisciplinario y difundan los resultados de sus estudios a través de responsables políticos y medios de comunicación. Por último, dicho organismo recomienda que los programadores informáticos proporcionen tecnologías que permitan actualizar de forma intuitiva las propiedades en materia de privacidad de datos y faciliten la protección de datos personales en proyectos de infraestructuras públicos conjuntos.

En Estados Unidos, la Comisión Federal de Comercio (FTC) hace hincapié en los principios prácticos y de procedimiento para la protección de la privacidad, en particular, el diseño basado en la privacidad, la selección simplificada del consumidor y los principios sustantivos y de procedimiento para garantizar la transparencia. La Comisión también destaca la protección de la privacidad del consumidor en organizaciones empresariales, así como con respecto a los productos y todas las etapas de desarrollo de los servicios.[161]

La Agencia Española de Protección de Datos (AEPD) ha publicado una guía sobre diseño basado en la privacidad en la que subraya la necesidad de tener en cuenta la privacidad y los principios de protección de datos desde el comienzo de todo tipo de procesamiento de datos. En la guía también se presentan principios y estrategias fundamentales para el procesamiento de datos personales.[162]

Cuadro 4 – Relación entre los objetivos en materia de privacidad y las estrategias de diseño basado en la privacidad

Objetivos de protección de la intimidad	Estrategias de protección de la privacidad orientadas a los datos	Estrategias de protección de la privacidad orientadas a los procesos
Disociación	Minimizar, abstraer, clasificar, ocultar	
Control		Controlar, hacer cumplir, demostrar
Transparencia		Informar

6.3 Conclusiones extraídas y medidas futuras

Los ciberataques, la fuga de datos y la utilización no autorizada de datos personales tienen lugar cada vez con más frecuencia. La comprensión de los derechos y las obligaciones de las personas y las organizaciones con respecto a la información personal reviste actualmente mucha más importancia que antaño, en particular en el caso de las organizaciones que procesan información que permite la identificación de personas.

En este capítulo se ha proporcionado una visión general de las modificaciones en el plano jurídico y las medidas técnicas de ciberseguridad relativas a la protección de datos personales implantadas en los Estados Miembros. También se han abarcado prácticas idóneas para ayudar a los Estados Miembros a adaptarse a la evolución de los requisitos de privacidad de datos y se ha abordado la función que desempeñan las tecnologías de ciberseguridad para mitigar los riesgos y fomentar la conformidad.

---

161 FTC. Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policy-makers, marzo de 2012.

162 Agencia Española de Protección de Datos (AEPD), Guía de Privacidad desde el Diseño, octubre de 2019.

Del examen de las distintas tecnologías de ciberseguridad y de las prácticas idóneas utilizadas por los Estados Miembros a los efectos de protección de la información personal cabe destacar las conclusiones siguientes:

- Los acuerdos institucionales para fomentar la pseudonimización y el diseño basado en la privacidad, entre otras medidas tecnológicas, contribuyen a crear un entorno más seguro.
- Las empresas que recopilan y utilizan información personal deben hacer todo lo posible para implantar medidas técnicas que permitan proteger mejor la información personal a nivel básico.
- Las partes interesadas, incluidos los interesados, la sociedad civil, las instituciones académicas y los representantes del sector industrial, deben abordar conjuntamente la utilización de la tecnología y esforzarse por aumentar la concienciación y mejorar la seguridad.

Capítulo 7 – El futuro de la Cuestión

La ciberseguridad reviste suma importancia para todas las partes interesadas, en particular los gobiernos y los consumidores. La labor del UIT-D en esa esfera contribuye a aumentar la concienciación en materia de riesgos. A raíz del aumento ininterrumpido de los índices de conectividad y utilización de Internet en todo el mundo, es necesario garantizar la protección de los consumidores y los sistemas. Habida cuenta de la necesidad de compartir información en todo el mundo sobre métodos de ciberseguridad, el equipo directivo de la Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D considera que la Cuestión sobre ciberseguridad debe mantenerse sin variaciones a lo largo del próximo ciclo de estudios. Los temas abordados durante dicho periodo de estudios siguen siendo pertinentes y deben constituir la base de nuevas contribuciones y trabajos durante el próximo periodo de estudios. En consecuencia, el marco general de la Cuestión no debería variar, y puesto que los problemas en materia de seguridad afectan a todas las tecnologías, la Cuestión 3/2 sigue siendo aplicable a todas las tecnologías nuevas e incipientes, incluidos los aspectos de diseño.

Anexos

Annex 1: List of contributions and liaison statements received on Question 3/2

Contributions on Question 3/2

Web	Received	Source	Title
2/407	2021-03-03	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/400	2021-03-01	United States	Update on Cyber Awareness Campaigns
2/385	2021-01-28	Bhutan	Survey findings on National Child Online Safety and Protection
RGQ2/278	2020-09-22	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
RGQ2/272	2020-09-22	United Kingdom	UK case study: Cyber resilience best practice for SMEs
RGQ2/268	2020-09-22	Republic of Korea	Protecting personal data in responding COVID-19 pandemic (Korea's experience)
RGQ2/261	2020-08-19	Togo	Draft text for Chapter 1 of the Final Report for Question 3/2 - Update on the status of spam and malware, including mitigation responses
RGQ2/241	2020-08-26	United Kingdom	Updated case study on securing consumer Internet of Things (IoT) devices in UK
RGQ2/235	2020-08-20	United Kingdom	UK Government Digital Service (GDS) Global Digital Marketplace Programme
RGQ2/234	2020-08-20	United Kingdom	UK case study - reporting service for phishing emails
RGQ2/216	2020-07-27	Brazil	Brazilian National Cybersecurity Strategy (E-Ciber)
RGQ2/215	2020-07-27	Brazil	#SafeConnection (#ConexãoSegura) Awareness Campaigns
RGQ2/214	2020-07-27	Brazil	Brazilian National Cyberdrill - Cyber Guardian Exercise
2/344	2020-02-11	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/342	2020-02-11	Republic of Korea	Korea's major amendment to data protection law and its implication

(continuación)

Web	Received	Source	Title
2/341	2020-02-11	Republic of Korea	Implementation plan for strengthening national cybersecurity of Korea
2/338	2020-02-11	Co-Rapporteur for Question 3/2	Draft table of contents (V1) for the Final Report of Q3/2
2/336	2020-02-11	United Kingdom	Case study of best practices for securing customer Internet of Things in the UK
2/331	2020-02-11	Keio University (Japan)	Proposed text for consideration of security issues for ICT accessibility
2/328	2020-02-08	Deloitte (United States)	People with disabilities and the Internet of Things
2/325	2020-02-08	Democratic Republic of the Congo	La sécurité numérique en République Démocratique du Congo
2/322	2020-02-07	Welchman Keen (Singapore)	Enhancing capacity and capability for critical national infrastructure in the Pacific Island Nations
2/321	2020-01-08	Sudan	WSIS project for consideration by Question 3/2
2/305	2020-01-15	Mexico	Perception on security and trust from Mexican users on fixed and/or mobile Internet
2/287	2020-01-07	China	Forum on network security technology development and international cooperation
2/286	2020-01-07	China	National Network Security Publicity Week and network security industrial park
2/272	2020-01-02	Niger	Cybersecurity best practices: case study and recommendation
2/264	2019-12-27	Russian Federation	Protecting children from information harmful to their health and development. Experience of the Russian Federation
RGQ2/TD/13 +Ann.1 (Rev.1)	2019-10-08	Forum of Incident Response and Security Teams (FIRST)	Introduction to incident response for policy makers
RGQ2/196	2019-09-24	Silensec Africa Limited (Kenya)	Using cloud-based cyber ranges and competence frameworks for the delivery of cyber drills
RGQ2/179	2019-09-23	China	China's practice in protecting children's personal information
RGQ2/175	2019-09-19	United Kingdom	Follow up to "case study for the use of Active Cyber Defence on UK Government networks"

(continuación)

Web	Received	Source	Title
RGQ2/156 +Ann.1-3	2019-09-04	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
RGQ2/155	2019-08-23	United Kingdom	Case study of best practices for ransomware risk mitigation in the UK
RGQ2/153 +Ann.1-2	2019-08-22	United States	Enhancing the resilience of the Internet and communications ecosystem against botnets and other automated, distributed threats
RGQ2/151	2019-08-22	United States	NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1
RGQ2/146	2019-08-21	Senegal	Overview of the National Cybersecurity School with a regional focus
RGQ2/143	2019-08-23	Brazil	The adoption of the Brazilian General Data Protection Law
RGQ2/135	2019-07-30	Bhutan	Cybersecurity initiatives in Bhutan
RGQ2/134	2019-07-29	State of Palestine, which participates in ITU under Resolution 99 (Rev. Dubai, 2018)	Government Data Exchange
RGQ2/118	2019-06-21	Democratic Republic of the Congo	Securing information and communication networks: Best practices for developing a culture of cybersecurity
2/201	2019-03-08	Côte d'Ivoire	Survey of online activities and Internet use by children in Côte d'Ivoire
2/199 (Rev.1)	2019-03-06	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/174	2019-02-07	Côte d'Ivoire	Mapping of cybercrime threats in Côte d'Ivoire
2/173	2019-02-07	Côte d'Ivoire	Presentation of Platform for Combatting Cybercrime (PLCC)
2/172	2019-02-07	NRD Cyber Security (Lithuania)	National and sectorial CSIRT developments as means to strengthen cybersecurity environments, 2019 update
2/168	2019-02-07	Republic of Korea	2019 Comprehensive Cybersecurity Plan for the private sector
2/167	2019-02-07	Symantec Corporation (United States)	The importance of cyber threat intelligence in the definition of national cybersecurity strategies
2/165	2019-02-06	Mexico	Fixed and/or mobile Internet users' perception of cybersecurity
2/156	2019-02-05	China	Work experiences in personal information protection

(continuación)

Web	Received	Source	Title
2/155	2019-02-05	China	Design of evaluation index for network security capability
2/154	2019-02-05	China	Experience of Internet governance with the coordinated participation of the whole of society
2/152	2019-02-01	Benin	Cybersecurity in the era of the digital economy in Benin
2/141	2019-01-15	Chad	Digital dividend
2/140	2019-01-15	Chad	Vulnerability of connected TVs
2/136	2019-01-15	Chad	Status of cybersecurity in the Republic of Chad
RGQ2/TD/1	2018-09-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for ITU members
RGQ2/79	2018-09-18	Bhutan	Challenges, issues and recommendations from Bhutan: developing country perspective
RGQ2/75	2018-09-18	Namibia	Enforcement of cyber security challenged by cloud services
RGQ2/55	2018-09-10	United Kingdom	Case study for the use of Active Cyber Defence on UK government networks
RGQ2/47	2018-08-31	BDT Focal Point for Question 3/2	Information on two publications issued in 2017: regional review of national activities on child online protection in Europe; and mobile identification: implementation, challenges, and opportunities
RGQ2/39 +Ann.1	2018-08-20	High-Tech Bridge SA (Switzerland)	Cybersecurity awareness and other educative activities to members
RGQ2/32	2018-08-16	Guardtime AS (Estonia)	Towards cyber resilience - the role of national cyber exercises
RGQ2/30	2018-08-15	Brazil	Survey proposal
RGQ2/26	2018-08-14	NRD Cyber Security (Lithuania)	National and sectoral CSIRT developments as means of strengthen cybersecurity environments
RGQ2/25	2018-08-14	Proge-Software (Italy)	Data Privacy and Cloud.be compliant
2/91	2018-04-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/84	2018-04-23	Japan	Proposal for workshops in 2018-2021 study period

(continuación)

Web	Received	Source	Title
2/82	2018-04-23	Iran University of Science and Technology (Islamic Republic of Iran)	KOVA Project: A best practice for COP implemented in Iran
2/75	2018-04-14	A.S. Popov Odessa National Academy of Telecommunications (Ukraine)	ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection. Conclusions and Recommendations
2/74	2018-04-13	Korea Telecom (Republic of Korea)	Study topics for Question 3/2 in the current study period
2/71	2018-04-11	G3ict	Spammers and phishers who target persons with disabilities
2/66	2018-04-08	Algérie Télécom SPA (Algeria)	Proposals on the content of the (Question 3/2) final report
2/49	2018-03-15	Burundi	Current situation with regard to the Burundian Penal Code in relation to efforts to combat cybercrime
2/41	2018-02-28	Burundi	Cybersecurity, Internet Exchange point and e-commerce in Burundi

Incoming liaison statements for Question 3/2

Web	Received	Source	Title
RGQ2/242	2020-08-31	Council Working Group on Child Online Protection	Liaison statement from the Council Working Group on Child Online Protection (CWG-COP) to ITU-D SG2 on the outcome of the 15th and 16th Meetings of CWG-COP
RGQ2/174	2019-09-18	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D SG2 Q3/2 on vulnerability of TVs
2/182 +Ann.1	2019-02-11	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D Study Group 2 Question 3/2 on Cybersecurity in Africa (overview and out-look), from Democratic Republic of Congo
RGQ2/62	2018-09-14	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D SG2 Q3/2 on collaboration and liaison representative with ITU-D Question 3/2
RGQ2/43	2018-08-27	ITU-T Study Group 13	Liaison statement from ITU-T SG13 to ITU-D SG1 Q3/1 and ITU-D SG2 Q3/2 on inter-sec-tor coordination
RGQ2/3	2018-05-11	ITU-T JCA-IMT2020	Liaison Statement from JCA-IMT2020 to ITU-D Study Groups 1 and 2 on invitation to update the information in the IMT2020 roadmap

(continuación)

Web	Received	Source	Title
2/73	2018-04-13	ITU-T JCA-AHF	Liaison Statement from ITU-T JCA-AHF to ITU-D Study Group 1 Q7/1 and Study Group 2 Q3/2 on JCA-AHF recent meeting reports
2/69	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on collaboration and liaison relationship with ITU-D Study Group 2 Question 3/2
2/68	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on best practices in Benin and Senegal
2/67 (Rev.1)	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on new work item X.framcdc "Framework of the creation and operation for a Cyber Defense Center"
2/62	2018-04-03	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Question 3/2 on new work item X.framcdc "Framework of the creation and operation for a Cyber Defense Center"
2/46	2018-03-05	ITU-T JCA-IMT2020	Liaison Statement from ITU-T JCA-IMT2020 to ITU-D study groups on invitation to update the information in the IMT2020 roadmap
2/23	2017-11-24	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Question 3/2 on an ongoing work item on technical framework for countering telephone service scam
2/10	2017-11-22	ITU-T Study Group 20	Liaison Statement from ITU-T SG20 to ITU-D study groups on work on the combat of counterfeit ICT devices and mobile device theft

Annex 2: List of lessons learned received on Question 3/2

Web	Received	Source	Title
SG2RGQ/272	2020-09-22	United Kingdom	UK case study: Cyber resilience best practice for SMEs

The UK Government provides targeted support to small and medium-sized enterprises (SMEs) to help them navigate complicated standards to better understand how to mitigate cyberrisk. This support is designed specifically for organizations who are not aware of the cyberthreat and have limited resources, both financially and in terms of technical capability. Lessons learned include the following:

- Clear and consistent cyberrisk management messaging is crucial. Critically, **awareness campaigns** should not just explain *what* businesses need to do and *how* they can actually carry out the action by pointing to government advice, guidance and support, but should draw attention to ***why*** they should do it.
- **Advice and guidance** is most effective when it is non-technical, size-specific and easy to access. Government and law enforcement should use national, regional and local networks, and work in partnership with key industry bodies, to identify levers and business touchpoints that can be used to amplify messaging, and ensure advice and guidance reaching SMEs.
- The creation of a government-backed **certification scheme** can be an effective intervention to support SMEs to improve their cybersecurity. The certification scheme can:
    - be quickly and effectively delivered by a single supplier if the government can outline the technical controls and/or minimum standards that should be covered;
    - evolve to continue to meet the needs of SMEs and address the changing threat landscape;
    - better ensure organizations remain compliant through having a certification expiry date and requiring annual recertification.

Web	Received	Source	Title
SG2RGQ/235	2020-08-20	United Kingdom	UK Government Digital Service (GDS) Global Digital Marketplace Programme

Challenges

A range of interconnected challenges face governments in relation to traditional approaches to public procurement of ICTs, which is typically:

- neither understanding nor meeting the needs of users
- task oriented, risk averse and inflexible
- isolated from what happens:
  - 'before' (strategic planning, investment appraisals, early market engagement)
  - 'after' (service delivery, monitoring and evaluation, supplier relationship management)
- hidden from public scrutiny due to the poor quality, inconsistency, incompleteness and poor availability of data.

User-centred design approaches

Since GDS was established in 2011, it has incubated, embedded and mainstreamed new standards-based approaches to government transformation.

These approaches were first conceptualized by the Government Design Principles,[163] published in April 2012.

Since then, GDS and the government and UK public sector more broadly have been incrementally applying these principles to redesign and improve services, organizational structures, governance approaches, etc. This includes public procurement.

Social Purpose Digital Commissioning

Focus on culture, mindset, collaboration and capability, by:

- understanding users' needs
- being clear about the problems you are trying to overcome (e.g. legacy ICT, system vulnerabilities, capability and capacity, governance and accountability, etc.) to meet users' needs
- being outcome-oriented (rather than solution-oriented), experimental and flexible, making small incremental investments to try out different approaches to address users' problems, learning quickly and iteratively
- being multidisciplinary and collaborative coalition builders, advocating for systemic change through communities of practice
- engaging throughout the end-to-end lifecycle of delivery - the 'before' and 'after' of procurement
- being open to public scrutiny through deliberative participation of civil society, enabled by structured, quality, consistent, complete and published open data.

[163] UK Government. Guidance. Government Design Principles. April 2012.

Web	Received	Source	Title
SG2RGQ/215	2020-07-27	Brazil	*#ConexãoSegura* (#SafeConnection) Awareness Campaigns

The campaign around personal data protection on the Internet reinforced the importance of telling consumers how to protect themselves in the digital environment. The interactions of consumers on digital media and on the website revealed that many of them have a number of doubts about what is fraud or scam - especially when it involves cash prizes, in addition to not knowing what to do when they are victims of these situations. It is also important to advise people not to post or publish personal data (surprisingly many people do not know what can happen). In the next initiative, it would be interesting to expand the dissemination of materials further in order to reach a wider audience.

Web	Received	Source	Title
SG2RGQ/214	2020-07-27	Brazil	Brazilian National Cyberdrill - Cyber Guardian Exercise

The exercise started with two national critical infrastructure (NCI) sectors and evolved in its second edition to a broader and more complex exercise process. The exercise continues to evolve, and for its third edition (cancelled due to the COVID-19 pandemic) it was planned to include six NCI sectors and to add an international cooperation component to the exercise.

Web	Received	Source	Title
2/325	2020-02-08	Democratic Republic of the Congo	La sécurité numérique en République Démocratique du Congo

Turn cybersecurity in the Democratic Republic of the Congo into a lever for integration, protection, good governance, economic growth and social progress.

This vision will make a significant contribution to building the country's capacity in its digital transformation (circulation of information, data economy, growth economy, transparency and traceability, interoperability of information systems, etc.). It will allow digitalization to become a key driver for modernizing the State, promoting economic growth and fostering social progress.

Web	Received	Source	Title
2/336	2020-02-11	United Kingdom	Case study of best practices for securing customer Internet of Things in the UK

A significant proportion of IoT devices do not have basic cybersecurity features built into them. Following 18 months of collaboration with industry and experts at the UK's National Cyber Security Centre (NCSC), the Department for Digital, Culture, Media and Sport (DCMS) published the Code of Practice (CoP) for Consumer IoT Security in October 2018. The 13 voluntary guidelines, as outlined in the 2018 CoP, provide a much-needed baseline for IoT devices that manufacturers should embed into their products to make them 'secure by design'.

These include:

- No default passwords
- Implement a vulnerability disclosure policy
- Keep software updated
- Securely store credentials and security-sensitive data
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure personal data are protected
- Make systems resilient to outages
- Monitor system telemetry data
- Make it easy for consumers to delete personal data
- Make installation and maintenance of devices easy
- Validate input data.

These guidelines are outcome-focused as opposed to being prescriptive, which gives companies the space to come up with innovative solutions and appropriate ways to secure their products. Some devices might require enhanced security that is not included on this list and, as such, retailers and manufacturers are encouraged to secure their devices accordingly and seek solutions beyond the 13 guidelines. Action on the first three guidelines will bring largest security benefits in the short term.

Web	Received	Source	Title
2/331	2020-02-11	Keio University (Japan)	Proposed text for consideration of security issues for ICT accessibility

This document describes the consideration and implementation of cybersecurity measures for persons with disabilities, especially those with hearing difficulties, such as telecommunication relay service and remote captioning, to enhance accessibility to information and communication services.

Web	Received	Source	Title
SG2RGQ/134	2019-07-29	State of Palestine	Government Data Exchange

The central server issues certificates to security servers and provides a list of authenticated certificates to the systems connected to the Government Data Exchange. In addition, the central security server maintains encrypted activity data (hash logs) from the security servers to enable a series of e-service uses to be built subsequently, if necessary. If one of the parties to the service denies sending or receiving certain information, the service provider and user logs are compared with the encrypted copy in the central server. This method allows the integrity of security server logs to be checked, as it is impossible to change the log without it subsequently being detected.

The terms of the data-sharing process are defined by a memorandum of understanding signed by the two parties sharing the data and the Ministry of Telecommunications and Information Technology (MTIT), as third-party system operator. The memorandum includes an annex on the obligations of the parties, an annex on controls, standards and the duties and rights of each party, and an annex on the data which the two parties agree to share.

The system allows a connected ministry to determine which other connected institutions may access and read its data and the level of data that may be accessed. This is done by means of a control window on the ministry's own security server, enabling it to grant access rights to any of its services to the institutions it wishes.

Encrypted data are shared directly through secure servers from one information system to another. They do not pass through the central system and cannot be displayed there. The central system only has statistical information on the data shared.

Using this approach, the system facilitates the secure sharing of data between institutions, enabling them to share data between one another. It has also made it easier for the public to access services currently available G2G, by only going to one institution where the service involves more than one. MTIT is currently working to develop this mechanism and to provide services to the public directly via applications being developed.

Web	Received	Source	Title
SG2RGQ/146	2019-08-21	Senegal	Overview of the National Cybersecurity School with a regional focus

- Enhancing international cooperation, particularly between developed and developing countries.
- The school's regional nature helps to enhance cooperation among African countries.
- Covering all aspects of cybersecurity in both initial and continuing training.
- As cybersecurity is a prerequisite for the Digital Senegal 2025 Strategy (SN2025), classes have begun at the offices of the National School of Administration (ENA) while construction of the school's own premises is being completed at Diamniadio, 20 km from Dakar.
- The school will be the final element in the system for information system security and cybersecurity already in place.
- Boosting the fight against cybercrime in Africa.

Web	Received	Source	Title
SG2RGQ/151	2019-08-22	United States	NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1

The recent update process to develop Version 1.1 of the Framework demonstrates an example of a good process for stakeholder engagement to ensure the Framework remains a useful tool for managing cybersecurity risk.

Web	Received	Source	Title
SG2RGQ/155	2019-08-23	United Kingdom	Case study of best practices for ransomware risk mitigation in the UK

A recent advisory on ransomware from the National Cyber Security Centre (NCSC) recommends the following risk-mitigation techniques:

- Keep devices and networks up to date (e.g. prompt updating and patching, and regular scans)
- Prevent and detect lateral movement in your enterprise network
- Segment networks
- Set up a security monitoring capability
- Whitelist applications
- Use antivirus
- Back up files.

The full advisory and detailed list of recommendations can be found at: https://www.ncsc.gov.uk/news/ongoing-threat-organisations-ransomware

Protecting your organization from ransomware: https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

Mitigating malware: https://www.ncsc.gov.uk/guidance/mitigating-malware

Unfortunately, it is not a question of 'if' but 'when' a cyberattack will occur. In the event an attack does take place, cooperation between the public and private sectors is key to understanding the threat and coordinating a quick and effective response to mitigate the impact of an attack. In the event of an attack, organizations are advised to contact the National Crime Agency, NCSC's Cyber Incident Response, or Cyber Security Information Sharing Partnership (CiSP). NCSC led the UK's response to the WannaCry attack and worked in collaboration with the National Crime Agency (NCA). Over the course of an incident, NCSC publishes statements and guidance for large organizations as well as home users and small businesses. Up-to-date information is announced via the NCSC Twitter account (@NCSC).

Web	Received	Source	Title
SG2RGQ/196	2019-09-24	Silensec Africa Limited (Kenya)	Using cloud-based cyber ranges and competence frameworks for the delivery of cyber drills

This contribution recommends the use of cyberrange technology (cloud-based – public or private cloud) and competency frameworks in the development and delivery of new generation cyberdrills.

Web	Received	Source	Title
2/201	2019-03-08	Côte d'Ivoire	Survey of online activities and Internet use by children in Côte d'Ivoire

- De-dramatize prevention by banishing the anxiety-provoking approach. Internet prevention can be part of a fear culture. However, this increases the anxiety of parents who are already worried about a technology they do not understand well, thereby undermining the extraordinary learning tool that is the Internet.
- Encourage educational programmes aimed at developing best practices in content management and raising children's awareness of responsible use of the Internet.
- Put an Internet portal online in order to provide children, adolescents, parents and teachers with an educational base.
- Involve all stakeholders in community-awareness activities: government agencies, the private Internet sector, NGOs, community groups and the general public.

Web	Received	Source	Title
2/174	2019-02-07	Côte d'Ivoire	Mapping of cybercrime threats in Côte d'Ivoire

Statistics should be collected on complaints and damages (financial, moral).

Web	Received	Source	Title
2/173	2019-02-07	Côte d'Ivoire	Presentation of Platform for Combating Cybercrime (PLCC)

- Development of partnerships between bodies responsible for combating cybercrime and the police in developing countries
- Awareness-raising in schools
- Collaboration with equivalent organizations in other countries.

Web	Received	Source	Title
SG2RGQ/26 2/172	2018-08-14 2019-02-07	NRD Cyber Security (Lithuania)	National and sectoral CSIRT developments as means to strengthen cybersecurity environments (2018 +2019 update)

For national digital security success, CSIRTs should focus substantial energy on broad facilitation for developing additional independent capabilities – in industries, professional communities, education centres, research, events, meet-ups and conferences, private and internal CSIRTs.

Web	Received	Source	Title
2/167	2019-02-07	Symantec Corporation (United States)	The importance of cyber threat intelligence in the definition of national cybersecurity strategies

- Establish and adopt situation awareness and threat intelligence policies.
- Develop incident analysis and response capabilities - establish CERTs.
- Develop collaboration with the private sector and information-sharing policies (public-private partnerships).

Web	Received	Source	Title
2/152	2019-02-01	Benin	Cybersecurity in the era of the digital economy in Benin

Benin calls on ITU-D Study Group 2 to support:

- the establishment of a national CERT in Benin to enhance the level of trust in cyberspace;
- the building up of a common African security and defence policy;
- the creation of a panel of eminent personalities to reflect on Africa's role in regard to security;
- the establishment of a CERT-AFR (for Africa) along the lines of CERT-EU (for the European Union);
- a coordinated effort to avoid disparities between the strategies adopted and means deployed by Member States in terms of military cyberdefence capabilities;
- regulators and ICT authorities as they seek to:
  - adopt measures designed to enhance the security of information systems and networks;
  - create reliable digital identities;
  - protect minors and vulnerable groups; and
  - foster transparency.

Web	Received	Source	Title
SG2RGQ/25	2018-08-14	Proge-Software [*SME pilot*] (Italy)	Data Privacy and Cloud - be compliant

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) (EU) 2016/679 governs data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying regulation within the EU. Superseding Data Protection Directive 95/46/EC, the regulation contains provisions and requirements pertaining to the processing of personally identifiable information (personal data) of individuals (formally called data subjects in the GDPR) inside the European Union, and applies to an enterprise that is established in the EU or – regardless of its location and the data subjects' citizenship – that is processing the personal data of people inside the EU. Controllers of personal data must put in place appropriate technical and organizational measures to implement the data-protection principles. Severe penalties are applied to violators.

Cloud computing

In computer science, cloud computing describes a type of outsourcing of computer services, similar to the way in which electricity supply is outsourced. Users can simply use it. They do not need to worry where the electricity is from, how it is made, or how it is transported. Periodically they pay for what they have consumed. The idea behind cloud computing is similar: The user can simply use storage, computing power or specially crafted development environments without having to worry how these work internally. Cloud computing is usually Internet-based computing. According to a paper published by IEEE Internet Computing in 2008, *"Cloud computing is a paradigm in which information is permanently stored in servers on the Internet and cached temporarily on clients that include computers, laptops, handhelds, sensors, etc."*.

Web	Received	Source	Title
SG2RGQ/32	2018-08-16	Guardtime AS [*SME pilot*] (Estonia)	Towards cyber resilience – the role of national cyber exercises

Cyberexercises are essential to achieving sustainable cyberresilience. Cyberexercises are different from training, and must be customized, realistic and engaging. Governments should consider developing a programme to govern cyberresilience, covering education, training and cyberexercises ranging from localized events to customized national-scale exercises conducted on a regular basis.

Web	Received	Source	Title
2/71	2018-04-11	G3ict	Spammers and phishers who target persons with disabilities

1) Contact the service provider to inform it of the highjacking of your e-mail address.
2) Try to give information on the spammer's/hacker's contact details with an example e-mail, e.g. by forwarding the suspect e-mail to its fraud section.
3) Ask to have your violated e-mail blocked.
4) Change your e-mail address.
5) Let your friends and contacts know you have been hacked and give them the new address.
6) Do not click on any web addresses unless you have verified it is in fact from a known source.

Web	Received	Source	Title
2/41	2018-02-28	Burundi	Cybersecurity, Internet exchange point and e-commerce in Burundi

Security of IT data and of communication networks in order to ensure high-quality services is the pillar of ICT-sector development. A legal and regulatory framework for cybersecurity in our country is an essential tool for implementing all aspects of data security. The introduction of an Internet exchange point facilitates local communications and reduces latency times and associated costs. Lastly, domain name management provides facilities for investors. Data security will thus enable us to ensure reliable e-transactions and retain our customers.

Unión Internacional de las Telecomunicaciones (UIT)
Oficina de Desarrollo de las Telecomunicaciones (BDT)
Oficina del Director
Place des Nations
CH-1211 Ginebra 20
Suiza
Correo-e: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Director Adjunto y Jefe del Departamento de Administración y Coordinación de las Operaciones (DDR)
Place des Nations
CH-1211 Ginebra 20
Suiza

Correo-e: bdtdeputydir@itu.int
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

Departamento de Redes y Sociedad Digitales (DNS)
Correo-e: bdt-dns@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Departamento del Centro de Conocimientos Digitales (DKH)
Correo-e: bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Departamento de Asociaciones para el Desarrollo Digital (PDD)
Correo-e: bdt-pdd@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

África

Etiopía
International Telecommunication Union (ITU)
Oficina Regional
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Adis Abeba
Ethiopía

Correo-e: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Camerún
Union internationale des télécommunications (UIT)
Oficina de Zona
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Camerún

Correo-e: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal
Union internationale des télécommunications (UIT)
Oficina de Zona
8, Route des Almadies
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar – Yoff
Senegal

Correo-e: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe
International Telecommunication Union (ITU)
Oficina de Zona
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe
Correo-e: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Américas

Brasil
União Internacional de Telecomunicações (UIT)
Oficina Regional
SAUS Quadra 6
Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul
(Anatel)
CEP 70070-940 Brasilia – DF
Brasil
Correo-e: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados
International Telecommunication Union (ITU)
Oficina de Zona
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados
Correo-e: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

Chile
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

Correo-e: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras
Correo-e: itutegucigalpa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

Estados Árabes

Egipto
International Telecommunication Union (ITU)
Oficina Regional
Smart Village,
Building B 147, 3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
El Cairo
Egipto

Correo-e: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacífico

Tailandia
International Telecommunication Union (ITU)
Oficina Regional
Thailand Post Training Center, 5th floor
111 Chaengwattana Road
Laksi
Bangkok 10210
Tailandia

Dirección postal:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Tailandia
Correo-e: ituasiapacificregion@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia
International Telecommunication Union (ITU)
Oficina de Zona
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonesia

Dirección postal:
c/o UNDP – P.O. Box 2338
Jakarta 10110, Indonesia
Correo-e: ituasiapacificregion@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322/2324
Fax: +62 21 389 55521

Países de la CEI

Federación de Rusia
International Telecommunication Union (ITU)
Oficina Regional
4, Building 1
Sergiy Radonezhsky Str.
Moscú 105120
Federación de Rusia

Correo-e: itumoscow@itu.int
Tel.: +7 495 926 6070

Europa

Suiza
Unión Internacional de las Telecomunicaciones (UIT)
Oficina Regional
Place des Nations
CH-1211 Ginebra 20
Suiza
Correo-e: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

Unión Internacional de Telecomunicaciones
Oficina de Desarrollo de las Telecomunicaciones
Place des Nations
CH-1211 Ginebra 20
Suiza

ISBN: 978-92-61-34103-9

Publicado en Suiza
Ginebra, 2021