Prácticas para garantizar la ciberseguridad

Periodo de estudios

2022-2025

Cuestión 3/2

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

Producto provisional para 2023

Resumen ejecutivo

La Conferencia Mundial de Desarrollo de las Telecomunicaciones, celebrada en Kigali en 2022, revisó el mandato de la Cuestión de Estudio 3/2, que se centra en el intercambio de experiencias sobre prácticas de ciberseguridad. Las amenazas a la ciberseguridad son una preocupación importante a nivel mundial, y la creciente dependencia de la tecnología conduce a la escalada de los riesgos y consecuencias de los ataques cibernéticos. Las prácticas de garantía de la ciberseguridad se han convertido en un elemento esencial para la protección de redes, sistemas y datos contra actividades maliciosas.

Este informe refleja las contribuciones y debates de las reuniones de la Cuestión 3/2, y de un taller dedicado a las prácticas para garantizar la ciberseguridad. A continuación, se presentan seis conclusiones clave de estas discusiones:

1) Los diferentes niveles de criticidad y riesgos requieren de diferentes niveles de seguridad. Las evaluaciones de riesgos pueden ayudar a determinar el nivel adecuado de garantía, teniendo en cuenta la sensibilidad de los datos y activos que se protegen, así como las consecuencias de una violación y el entorno de amenazas.
2) La colaboración con las organizaciones asociadas, la industria y las múltiples partes interesadas puede ser una forma eficaz de impulsar la garantía de la ciberseguridad. La cooperación entre formuladores de políticas, organizaciones de la sociedad civil y la industria puede impulsar la demanda de seguridad e informar el desarrollo de políticas y reglamentación.
3) Considerar un enfoque reglamentario evolutivo, basado en el diálogo y la consulta. Las prácticas de garantía de la ciberseguridad pueden introducirse de manera voluntaria antes de convertirse en obligatorias, dependiendo de la necesidad de medidas más estrictas de protección contra los ciberataques.
4) Habida cuenta del panorama dinámico de las amenazas y la evolución de los riesgos de ciberseguridad, las prácticas para garantizar la ciberseguridad deben revisarse y adaptarse con el tiempo. Las auditorías internas periódicas y la suscripción a la inteligencia de amenazas se consideran prácticas idóneas.
5) Se están haciendo esfuerzos para educar a los consumidores y fabricantes sobre la importancia de la ciberseguridad y los beneficios de elegir productos más seguros. Los esquemas de etiquetado de ciberseguridad y las campañas de sensibilización pueden ayudar a informar a los usuarios sobre la seguridad de los productos tecnológicos.
6) Los acuerdos de reciprocidad pueden ayudar a facilitar la conformidad para los actores industriales que operan en múltiples mercados, mientras que la armonización de los requisitos de seguridad básicos reduce la carga reglamentaria sobre los proveedores de productos y servicios.

Introducción

Durante la última Conferencia Mundial de Desarrollo de las Telecomunicaciones, celebrada en Kigali (Rwanda) en junio de 2022, se examinó el mandato de la Cuestión de Estudio 3/2 – Seguridad en las redes de información y comunicación: Prácticas idóneas para el desarrollo de una cultura de ciberseguridad, y uno de los temas de estudio específicos era "compartir experiencias sobre prácticas de ciberseguridad"[1].

En el mandato aprobado para la Cuestión de Estudio 3/2 se reconoce que las amenazas a la ciberseguridad siguen siendo una preocupación importante para los gobiernos, las organizaciones y las personas de todo el mundo. Con la creciente dependencia de la tecnología, los riesgos y consecuencias potenciales de los ataques cibernéticos también están aumentando, y los ataques cibernéticos son cada vez más rentables[2]. Los ciberdelincuentes están operando un negocio lucrativo que se estima que costará 8 billones USD en todo el mundo[3].

Las prácticas para garantizar la ciberseguridad[4] se han convertido en un elemento esencial para la protección de redes, sistemas y datos contra actividades maliciosas. En líneas generales, se refieren a los procedimientos utilizados para garantizar que se aplican los controles pertinentes para la protección de la confidencialidad, integridad y disponibilidad de los dispositivos, sistemas, redes y datos electrónicos. Si bien no previenen directamente los ataques cibernéticos, su objetivo, si se implementan correctamente, es minimizar el riesgo de estos ataques. Las prácticas de garantía de la ciberseguridad pueden contrastarse con los controles, directrices y normas de seguridad específicos y pueden ser impuestas por reglamentos o adoptadas voluntariamente por la industria. Sin embargo, no existe un enfoque único para todos, ya que las autoridades nacionales y los reguladores del sector a menudo utilizan prácticas diferentes, desde autoevaluaciones y directrices voluntarias hasta sistemas de etiquetado y controles rígidos de cumplimiento.

Si bien no hay un único enfoque recomendado, es evidente que en los últimos años y meses se ha producido un movimiento sostenible hacia la adopción de prácticas para garantizar la ciberseguridad en todo el mundo, con diferentes evoluciones en varios países y regiones. Como ejemplo de este impulso, la Organización de Cooperación y Desarrollo Económicos lanzó en diciembre de 2022 la Recomendación del Consejo sobre la Seguridad Digital de los Productos y Servicios, que recomienda la adopción de políticas para mejorar la seguridad digital de los productos y servicios que sean proporcionales al riesgo, comenzando con un enfoque moderado basado en medidas políticas voluntarias y estudiar la necesidad de adoptar medidas obligatorias[5].

En el presente Informe se reflejan las contribuciones y los debates de las reuniones de la Cuestión de Estudio 3/2 y del Taller sobre prácticas de garantía de la ciberseguridad. El taller público de un día completo, celebrado en Ginebra el 23 de mayo, brindó la oportunidad de explorar el panorama global para garantizar la ciberseguridad en varios dominios (Internet de las cosas (IoT), telecomunicaciones, etc.) mostrando una variedad de prácticas y voces en curso de todo el mundo. Reunió a Estados Miembros y representantes de la industria, las autoridades técnicas y la sociedad civil.

El Equipo de Gestión de la Cuestión 3/2 desea aprovechar esta oportunidad para dar las gracias a todos los oradores y colaboradores por sus valiosas contribuciones a este tema. Este esfuerzo no sería posible sin su compromiso.

Habida cuenta de las valiosas aportaciones recibidas, este informe transmite principalmente los desafíos encontrados, el impacto evaluado y las lecciones aprendidas hasta la fecha al considerar y aplicar prácticas para garantizar la ciberseguridad mediante la presentación de seis conclusiones.

Estas conclusiones pueden constituir una aportación importante para los Miembros de la UIT a fin de evaluar sus prácticas existentes y evaluar la necesidad de adoptar enfoques adicionales o diferentes, teniendo en cuenta las experiencias y lecciones aprendidas por otras administraciones y organizaciones.

Conclusión 1: Los diferentes niveles de criticidad y riesgos requieren diferentes niveles de seguridad

Al considerar la aplicación de prácticas para garantizar la ciberseguridad, es crucial determinar en primer lugar lo que una entidad está tratando de proteger y los riesgos a los que se enfrentan los activos identificados. Los países y las empresas que desean protegerse contra los ciberataques deben, con carácter prioritario, identificar qué sistemas y activos necesitan protección y evaluar sus vulnerabilidades. En este sentido, disponer de un plan para realizar evaluaciones de riesgos es una herramienta útil. Uno de los marcos más conocidos es el Marco de Ciberseguridad del Instituto Nacional de Normalización y Tecnología (NIST)[6], actualmente en proceso de actualización[7], que ofrece un enfoque ampliamente utilizado para ayudar a determinar y minimizar los riesgos organizacionales. Establece directrices no reglamentarias que permiten a las organizaciones de todo el mundo identificar su propio panorama de riesgos y aplicar los controles de ciberseguridad adecuados en relación con éste. El marco revisado, que se finalizará a principios de 2024, se basa en un compromiso amplio y a largo plazo con la comunidad de partes interesadas que utilizan estas directrices, así como en la alineación continua con otras normas internacionales.

---

1 https://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/reference/SG2/ToR/Q3-2.aspx#Question

2 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090023PDFE

3 https://www.einnews.com/pr_news/606505844/cybercrime-damages-to-cost-the-world-8-trillion-usd-in-2023

4 La seguridad operacional está estrechamente ligada a las prácticas para garantizar la ciberseguridad, en el sentido de que la seguridad operacional puede constituir una buena base para las prácticas de aseguramiento. Broadcom, Vicepresidente de la CE 17 del UIT-T, presentó el modelo de buenas condiciones destacando que está compuesto por cuatro elementos clave: personas y procesos, conocimiento, productos de seguridad (seguridad exógena) y seguridad de los activos (seguridad endógena). Véase "Reducir el riesgo y proteger la reputación", https://www.itu.int/md/T22-SG17-C-0214/es

5 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481

6 https://www.nist.gov/cyberframework

7 https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

En el taller, el representante del NIST destacó que la posición beneficiosa de la organización como agencia no reguladora ha permitido un compromiso más profundo con las partes interesadas de la industria de todo el mundo para comprender los desafíos reales y recibir comentarios, que se han incorporado a las nuevas directrices[8]. Estos están destinados a ser adaptables y flexibles, y aplicables a todas las organizaciones y sectores. BitSight, un miembro del sector privado en el Sector UIT-D, habló sobre su plataforma, que integra el Marco de Ciberseguridad NIST y ha sido utilizada por varias agencias gubernamentales responsables de la ciberseguridad (como los Equipos de Intervención en caso de Emergencia Informática (EIEI), agencias nacionales de ciberseguridad, reguladores de telecomunicaciones)[9]. A través de la plataforma, los países pueden realizar evaluaciones de riesgos de sus infraestructuras y activos considerados esenciales y medir sus factores de riesgo.

Las evaluaciones de riesgos también pueden ayudar a determinar qué nivel de garantía es apropiado teniendo en cuenta la sensibilidad de los datos y activos protegidos, las consecuencias que tendría una violación y el entorno de amenaza (es decir, si una entidad es susceptible de sufrir un ciberataque). En algunos casos, los niveles de garantía vendrán dictados por requisitos reglamentarios. Cuanto mayor sea el nivel de garantía, más estrictos serán los controles de seguridad. Por ejemplo, un nivel bajo de garantía requeriría una contraseña del sistema o un cortafuegos, mientras que un nivel de garantía más alto requeriría la adición de controles más avanzados, como el cifrado avanzado y la autenticación multifactor.

Si bien las prácticas para garantizar la ciberseguridad aumentan los presupuestos de la tecnología de la información, no implementar controles de seguridad puede ser más costoso. Durante el taller, los representantes instaron a la audiencia a pensar en los costos de sufrir un ataque cibernético no sólo en términos financieros, ya que el costo adicional para la reputación puede ser mucho más perjudicial. Perder la confianza de los clientes y los ciudadanos tiene un efecto a largo plazo que se extiende más allá del dinero y las organizaciones deben ser capaces de entenderlo estratégicamente. Del mismo modo, para el sector público, los ataques exitosos pueden afectar la prestación de servicios públicos y actividades críticas, cuya interrupción tampoco puede evaluarse sólo en términos financieros, ya que afecta la vida de los ciudadanos.

Conclusión 2: Comprometerse con organizaciones asociadas, la industria y múltiples partes interesadas puede ser una forma efectiva de impulsar la garantía de ciberseguridad

En primer lugar, es importante comparar las iniciativas con otras, comprender las mejores prácticas y aprender de los éxitos y errores de otros durante el desarrollo de las iniciativas. En segundo lugar, es importante comprometerse con múltiples partes interesadas, incluida la industria, para obtener información importante para la iniciativa en sí como parte del desarrollo.

Aunque en los países menos adelantados las prácticas para garantizar la ciberseguridad sean cada vez más necesarias, pueden ser aún difíciles de aplicar. El representante de Cyber Defense Africa (CDA) en Togo explicó las dificultades que plantea el mercado local para garantizar la ciberseguridad en los Operadores de Servicios Esenciales (OSE)[10]. Se citaron factores a los que hay que hacer frente la falta de financiación, la falta de confianza en el gobierno como proveedor de servicios y la falta de capacidad e instalaciones humanas locales. Para ayudar a los Operadores de Servicios Esenciales a cumplir los controles de ciberseguridad recientemente publicados, el Gobierno de Togo creó una alianza público-privada con un gran proveedor de ciberseguridad de renombre para proporcionar servicios de ciberseguridad en los sectores público y privado. A través de este modelo, Togo creó Cyber Defense Africa (CDA) como un proveedor local de ciberseguridad autosuficiente y de alta calidad para apoyar a los Operadores de Servicios Esenciales (ESOs) sin carácter obligatorio. El modelo autosuficiente utilizado permitió a Togo reducir los numerosos problemas mencionados y comenzar a fomentar el talento local en el ámbito de la ciberseguridad, así como a impulsar el desarrollo del mercado local. El representante señaló la importancia de la CDA como entidad privada en un mercado competitivo a fin de garantizar la adaptabilidad, la alta calidad de los servicios y la fijación de precios competitivos.

También es importante fomentar la cooperación entre los responsables políticos que pueden establecer el entorno reglamentario y las organizaciones de la sociedad civil que pueden aumentar la demanda de seguridad, así como fundamentar el desarrollo de políticas y reglamentación sobre la base de las prácticas regionales e internacionales existentes e identificadas. Por ejemplo, la DiploFoundation es una organización internacional que ofrece programas de formación, creación de capacidades a gobiernos, reguladores, empresas y la sociedad civil sobre cuestiones de actualidad relacionadas con la ciberseguridad, y participa en el Diálogo de Ginebra sobre el comportamiento responsable en el ciberespacio (Diálogo de Ginebra)[11]. En 2020, el Diálogo de Ginebra produjo una colección de prácticas idóneas que incluye definiciones sugeridas de diseño seguro y gestión de vulnerabilidades, modelado de amenazas, seguridad de terceros y de la cadena de suministro, desarrollo seguro, gestión y divulgación de vulnerabilidades, así como cultura institucional[12]. El Global Forum on Cyber Expertise (GFCE) es una plataforma internacional que apoya la coordinación de proyectos, promueve el intercambio de conocimientos y experiencias, hace coincidir las solicitudes con ofertas de apoyo a la creación de capacidad y el desarrollo de proyectos de investigación[13]. El GFCE estableció cuatro centros regionales: en las islas del Pacífico, en África, en América y el Caribe, y en el sudeste asiático. Dada su presencia mundial y el diverso apoyo prestado por los países en desarrollo, el Foro está en condiciones de aportar opiniones regionales

[8] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090017PDFE
[9] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090024PDFE
[10] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090025PDFE
[11] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090020PDFE
[12] https://genevadialogue.ch/goodpractices/
[13] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090021PDFE

más diversas sobre las necesidades y demandas de la cibercapacitación. El GFCE tiene un portal en línea que sirve de repositorio de los proyectos implementados y en curso en materia de cibercapacitación a nivel mundial, así como de recursos y herramientas. Este portal también contribuye a reducir la duplicación de esfuerzos y ayuda a identificar algunos programas o lagunas y pautas en la prestación de servicos de fomento de la capacidad.

Conclusión 3: Considerar un enfoque regulatorio en evolución, informado a través del diálogo y las consultas

En muchos casos, las prácticas para garantizar la ciberseguridad se introducirán como voluntarias antes de convertirse en obligatorias. El cambio generalmente ocurre cuando los gobiernos consideran que la industria no está haciendo lo suficiente para asegurar los productos y que los consumidores no necesariamente tienen el conocimiento para evaluar si los productos son seguros o no. Esto puede llevar a los gobiernos y autoridades nacionales a actuar y estipular prácticas de aseguramiento que esperan que cumpla la industria. Por ejemplo, en Brasil, el regulador de las telecomunicaciones, Anatel, ha creado en el país un sistema de organismos de certificación y laboratorios de pruebas para la certificación de Equipos en las Instalaciones del Cliente (CPE o las pasarelas domésticas). Tradicionalmente, Anatel ha optado por proporcionar directrices voluntarias sobre ciberseguridad para el sector de las telecomunicaciones. Sin embargo, al realizar evaluaciones de riesgos se identificó que las recomendaciones no eran suficientes para los CPE, considerando las vulnerabilidades y amenazas asociadas a este tipo de equipos, y que era necesario establecer requisitos mínimos de seguridad obligatorios para estos productos. Dichos requisitos obligatorios para los proveedores de servicios de comunicación (PSC) se publicaron a principios de 2023 y se centran en vulnerabilidades como contraseñas no seguras y partes de servicio habilitadas innecesariamente. Los requisitos entrarán en vigor a principios de 2024 como parte de las pruebas de laboratorio obligatorias para la aprobación del producto[14]. Anatel explicó que la evolución de un enfoque no obligatorio a un requisito de certificación obligatoria de la ciberseguridad para un conjunto específico de equipos sólo era posible si se mantenía un amplio debate con el sector.

Del mismo modo, la Agencia Nacional de Ciberseguridad (NCA) del Reino de Arabia Saudita presentó su iniciativa para construir un Ecosistema[15] de Verificación y Validación Independiente (IV&V) para probar y certificar productos desde una perspectiva para garantizar la ciberseguridad a nivel nacional en Arabia Saudita. Además, la iniciativa tiene como objetivo identificar y clasificar los hardware y software que sean altamente sensibles a los riesgos y amenazas cibernéticos. También busca contribuir al desarrollo de capacidades humanas en IV&V. La iniciativa de la hoja de ruta considera comenzar con un programa voluntario antes de convertirlo en una obligación. La autoridad también mencionó la importancia de que dicho ecosistema finalmente se convierta en "autosostenible", lo que alimentó el enfoque adoptado por la NCA para alentar a las partes interesadas del mercado a realizar dichas evaluaciones.

En el ámbito de la seguridad de IoT, el Reino Unido también presenta un estudio de caso sobre la evolución de un enfoque voluntario a un enfoque obligatorio. En los últimos años, el Reino Unido ha decidido exigir, mediante legislación, un requisito de seguridad básico para los productos de consumo de IoT basado en la norma del Instituto Europeo de Normas de Telecomunicaciones (ETSI) EN 303 645, la primera norma de ciberseguridad aplicable a nivel mundial para dispositivos IoT de consumo. En el Reino Unido, los fabricantes, importadores y distribuidores tendrán que cumplir con tres de las 13 directrices de seguridad de ETSI, y la ley otorga poderes al gobierno para adoptar requisitos adicionales si es necesario, dependiendo de las evaluaciones periódicas de amenazas. La decisión de imponer una base de requisitos de seguridad se tomó tras un periodo de adopción voluntaria. En 2018, el país formuló un código de prácticas voluntario[16] para la seguridad de la IoT del consumidor, pero el cumplimiento de la industria no fue el esperado. La evidencia recopilada a través de ejercicios de consulta mostró que los consumidores valoran la seguridad y están dispuestos a pagar un exceso de precio por productos seguros. Sin embargo, las amenazas de seguridad no están sujetas al mismo nivel de regulación robusta que la seguridad del producto, lo que lleva a una falta de transparencia por parte de los fabricantes y a una adopción más lenta de las políticas de seguridad. La evidencia también encontró que el mercado de productos conectables al consumidor desincentiva la adopción de características básicas de seguridad, ya que los consumidores asumen abrumadoramente que los productos ya son seguros. El régimen tiene como objetivo abordar esta brecha imponiendo elementos del código de prácticas para garantizar que los fabricantes sean conscientes de las vulnerabilidades y tomen medidas para mitigarlas. El régimen Product Security and Telecommunications Infrastructure (PSTI) entrará en vigor en abril de 2024 y se aplicará a cualquier producto de consumo que pueda conectarse a Internet[17].

Uno de los desafíos identificados es el posible impacto en las pequeñas empresas y las microempresas que pueden enfrentar dificultades para cumplir con el nuevo régimen. La autoridad encargada del cumplimiento del Reino Unido está elaborando directrices para mitigar cualquier impacto desproporcionado. Además de trabajar con la industria, el Reino Unido compartió que los tres requisitos principales que se exigirán en el esquema se han identificado y comunicado de manera transparente durante varios años. A lo largo de los años, el Reino Unido ha realizado ejercicios sobre el proceso de implementación del régimen, incluidos los requisitos de contraseña, la arquitectura fundamental del producto, la exposición a la vulnerabilidad y los requisitos de transparencia de seguridad. La evaluación de impacto ha mostrado que se espera que los beneficios globales de reducir el volumen de ciberataques a consumidores y empresas superen los costos asociados con el régimen. Dado que la Ley Product Security and

[14] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090018PDFE
[15] https://nca.gov.sa/en/news?item=535
[16] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf
[17] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090014PDFE

Telecommunications Infrastructure (PSTI) 2022 es la primera legislación obligatoria sobre productos de ciberseguridad en el mundo, el costo de hacer cumplir el régimen es incierto, pero las estimaciones iniciales sugieren que los fondos asignados serán suficientes.

En algunos casos, la diferencia entre si una práctica de aseguramiento ha sido obligatoria o mantenida voluntaria está dictada por quién es el usuario o cliente. Por ejemplo, la República de Corea lanzó su Programa de Garantía de Seguridad en la Nube (CSAP), una certificación de seguridad para servicios de computación en la nube[18]. En general, esta certificación es voluntaria. No obstante, los clientes del sector público (es decir, las agencias públicas) deben utilizar un servicio en la nube que haya obtenido la certificación CSAP de conformidad con la reglamentación pertinente y, por tanto, los proveedores de servicios en la nube deben obtener la certificación cuando prestan servicios en la nube a organismos públicos.

Conclusión 4: Dado el panorama dinámico de amenazas y la evolución de los riesgos de ciberseguridad, las prácticas para garantizar la ciberseguridad no pueden ser estáticas y deben revisarse y adaptarse con el tiempo

La realización de auditorías internas periódicas que pueden ayudar a identificar deficiencias en los controles y el riesgo de exposición, así como la suscripción a la inteligencia de amenazas, se consideran prácticas idóneas. Incluso si un producto está certificado, podría, a lo largo de su ciclo de vida, sufrir fallas de seguridad. Los planes de certificación requieren la presentación de información en un momento específico, por lo que el proceso no tiene en cuenta los cambios dinámicos de las amenazas en el futuro. Un estudio reciente de BitSight mostró una fuerte correlación entre una mala "cadencia de parches" para las vulnerabilidades y la probabilidad de experimentar un incidente de ciberseguridad[19], señalando la importancia crítica de actualizar los sistemas tan pronto como estén disponibles los parches de seguridad, teniendo en cuenta la diferente distribución de parches en todo el mundo.

Las pruebas de penetración, o "pen-testing", son un ejercicio de garantía de seguridad que ayuda a evaluar la seguridad de un sistema de TI e identificar vulnerabilidades que de otro modo podrían utilizarse para explotar sistemas. OFCOM, el regulador de comunicaciones del Reino Unido, ejecuta voluntariamente con los proveedores de telecomunicaciones el esquema TBEST, una prueba de penetración que tiene como objetivo estimular un ataque cibernético para identificar vulnerabilidades de seguridad que luego, a través de un proceso de remedio, pueden abordarse para mejorar la postura de seguridad de la red de los operadores[20]. En la contribución se ofrece una reseña del proceso y las distintas partes interesadas implicadas. De manera más general, este plan es un ejemplo del enfoque de supervisión que está adoptando OFCOM, en el que se hace hincapié en la importancia de establecer relaciones de colaboración con la industria regulada por dicha autoridad. Hasta la fecha, todos los proveedores de comunicaciones del Reino Unido se han sometido o están aplicando el esquema TBEST voluntariamente y han implementado cambios como resultado. TBEST no constituye una "norma" ni un proceso de certificación. El objetivo consiste en permitir a los proveedores de servicios de comunicación tomar conciencia de las amenazas a la ciberseguridad e implementar los cambios apropiados de manera oportuna para mejorar sus capacidades de defensa en esta materia. Al conocer y abordar dichas vulnerabilidades y debilidades, los operadores se encuentran en una posición mucho más fuerte para proteger sus redes.

Conclusión 5: Se están haciendo esfuerzos para educar a los consumidores y fabricantes sobre la importancia de la ciberseguridad y los beneficios de elegir productos más seguros

Se han hecho esfuerzos para educar al público sobre la importancia de la ciberseguridad y las ventajas de elegir productos más seguros.

Un enfoque en este sentido es el desarrollo de un sistema de etiquetado de ciberseguridad (CLS) que, como ejemplifica Singapur, los productos certificados pueden ir acompañados de una etiqueta. Los sistemas de etiquetado sirven principalmente como una herramienta informativa para los consumidores. La Agencia de Ciberseguridad de Singapur (CSA) examinó un sistema de etiquetado de ciberseguridad cuyo objetivo es ayudar a los consumidores a distinguir entre dispositivos IoT más o menos seguros[21]. El sistema es voluntario (con la excepción de los enrutadores Wi-Fi, para los cuales es obligatorio) y tiene cuatro niveles, siendo el nivel 1 la base de seguridad. Los niveles 1 y 2 se basan en la autoevaluación de los fabricantes y los niveles 3 y 4 implican la evaluación de terceros por parte de un laboratorio aprobado. El sistema es multinivel para incentivar a los fabricantes a incorporar medidas de seguridad adicionales a los requisitos básicos. La CSA también discutió las compensaciones involucradas en exigir estándares de ciberseguridad, incluido el riesgo de que los fabricantes pasen por alto el mercado debido al aumento de los costos de cumplimiento. En cambio, el objetivo es cambiar la mentalidad de los fabricantes para ver la ciberseguridad como un habilitador y diferenciador del mercado en lugar de un costo. En lo que respecta a las repercusiones de un sistema de etiquetado de la ciberseguridad en Singapur, todavía se encuentra en una fase temprana del proceso y se están realizando esfuerzos para alentar a los fabricantes a participar en el plan y mejorar su ciberseguridad. En el futuro se llevará a cabo de nuevo una encuesta pública para evaluar la sensibilización y el comportamiento de los consumidores. El costo del cumplimiento se minimiza para los fabricantes en los niveles 1 y 2, y no ha habido un aumento significativo en el costo de los productos para los consumidores. Con el sistema voluntario, se espera que las fuerzas del mercado impulsen mejoras en la ciberseguridad entre los fabricantes.

[18] https://isms.kisa.or.kr/main/csap/intro/index.jsp
[19] https://www.bitsight.com/press-releases/study-finds-significant-correlation-between-bitsight-analytics-and-cybersecurity
[20] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/network-security-and-resilience/our-work
[21] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090016PDFE

Más allá de las etiquetas, es tan importante invertir en controles técnicos como en crear conciencia y educar a la población sobre los riesgos de ciberseguridad a los que se enfrentan las organizaciones y los países. Actualmente, los ataques de secuestro de software son la tendencia más preocupante. Para este tipo de ataques, el principal vector de ataque, es decir, la forma en que un delincuente ingresa a una red o sistema es a través de correos electrónicos de suplantación de identidad[22]. En el contexto, los ciberdelincuentes a menudo pueden eludir los controles de seguridad simplemente haciendo clic en un correo electrónico de suplantación de identidad. Por lo tanto, es crucial para garantizar la ciberseguridad concienciar a los ciudadanos y a los empleados sobre estos temas.

Conclusión 6: Es importante buscar acuerdos internacionales de sinergia/armonización y reciprocidad

La existencia de acuerdos de reciprocidad entre los modelos de garantía de la ciberseguridad, a saber, los sistemas de certificación y etiquetado, puede ser determinante para la ampliación de estas prácticas. Como destacaron las partes interesadas, los acuerdos de reciprocidad pueden ayudar a facilitar el cumplimiento para los actores industriales que operan en múltiples mercados. Sin embargo, habida cuenta de que los acuerdos de reciprocidad son un mecanismo formal que tiene muchas restricciones nacionales y que lleva tiempo aprobar y firmar, es necesario que las prácticas de garantía de la ciberseguridad encuentren sinergias con los enfoques internacionales existentes que estén en consonancia con las necesidades y prioridades nacionales. Esto reducirá la carga reglamentaria sobre los proveedores de productos y servicios con el fin de evitar requisitos contradictorios.

La CSA destacó la importancia de la colaboración internacional en el desarrollo y la aplicación de su sistema de etiquetado de ciberseguridad. Singapur ha firmado acuerdos de reconocimiento mutuo con Finlandia y Alemania, y está trabajando para ampliar sus asociaciones en esta área. Singapur reflexionó sobre su experiencia y compartió que los gobiernos deben ser proactivos en el establecimiento del reconocimiento, aunque los fabricantes también tienen interés en apoyar el proceso de reconocimiento, ya que reduce la carga de las pruebas y certificaciones repetidas, así como el acceso al mercado, en diferentes jurisdicciones. El proceso implica reunir a las partes interesadas para armonizar los requisitos y establecer normas comunes que sean realistas y no excesivamente onerosas.

A nivel europeo, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) tiene el mandato de desarrollar tres sistemas de certificación que tendrían reconocimiento en todo el mercado interior, por lo que tendrían un "reconocimiento mutuo" automático en toda la Unión Europea (UE). Esos sistemas son: el plan de criterios comunes de la UE para los productos de TIC, cuya ley se está preparando con miras a su adopción; el sistema de servicios en la nube, objeto de amplios debates y, por último, el sistema 5G, que se está desarrollando[23].

Además de la reciprocidad, y teniendo en cuenta los mercados internacionales en los que opera la industria, la armonización de los requisitos de seguridad básicos es también una consideración importante. Las normas del ETSI sobre productos de consumo IoT son un ejemplo de este esfuerzo. La pregunta principal es hasta qué punto los diferentes marcos reglamentarios estarán armonizados y hasta qué punto estarán conectados a través de las mismas normas internacionales. A este respecto, en el taller se señaló que fortalecer e incluso encontrar el lugar adecuado para el diálogo era un desafío. En lo que respecta a la armonización, las actividades de ENISA en materia de normalización de la ciberseguridad y 5G requieren la colaboración de CEN, CENELEC, ETSI, ISO/CEI, GSMA, 3GPP y GlobalPlatform. Uno de los principales resultados de la Agencia ha sido la consolidación de los controles de seguridad 5G de diferentes organismos de normalización en un solo repositorio[24].

[22] Una táctica común utilizada por los ciberdelincuentes para engañar a las personas para que revelen información confidencial o descarguen programa malicioso que infecta el sistema/red objetivo.

[23] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090019PDFE

[24] https://www.enisa.europa.eu/about-enisa/about/es

Anexo: Ejemplos de prácticas de garantía de la ciberseguridad

País u organización	Nombre de la práctica	Tipo de práctica	Alcance de la práctica	Tipo de enfoque	Referencia
Australia	Directrices para la seguridad por diseño de la IoT para fabricantes	Orientación	IoT	Voluntario	Enlace
Australia	Código de práctica: protección de la Internet de las cosas para los consumidores	Código de práctica	IoT	Voluntario	Enlace
Brasil	Ley 77/2021 Requisitos de ciberseguridad para equipos de telecomunicaciones	Requisitos para el plan de certificación	Equipos de telecomunicaciones	voluntario	Enlace
Brasil	Ley 2436/2023 – Requisitos mínimos de ciberseguridad para la evaluaciónd e la conformidad de los equipos en los locales del cliente (CPE)	Requisitos para el plan de certificación	CPE	Obligatorio	Enlace
Reino de Arabia Saudita	Verificación y validación independientes (IV&V)	Pruebas y certificación de productos. Identificación y clasificación de dispositivos y software	Productos	Inicialmente voluntario	Enlace
Corea (República de)	Programa de garantía de seguridad de la nube (CSAP)	plan de certificación	Nube	Combinado – generalmente voluntario. Obligatorio para la prestación de servicios en la nube a organismos públicos.	Enlace
Singapur	Plan de etiquetado de ciberseguridad	Plan de certificación y etiquetado	IoT	Combinado – generalmente voluntario. Obligatorio sólo para los encaminadores Wi-Fi domésticos.	Enlace
Reino Unido de Gran Bretaña e Irlanda del Norte	Régimen de seguridad de productos e infraestructura de telecomunicaciones (seguridad de productos)	Requisitos de seguridad mínimos	Productos conectables	Obligatorio	Enlace
Reino Unido de Gran Bretaña e Irlanda del Norte	Plan TBEST	Pruebas de penetración	Redes de telecomunicaciones	Voluntario	Enlace

ITUPublicaciones
Publicado en Suiza, Ginebra, 2023

Unión Internacional de Telecomunicaciones
Place des Nations, CH-1211 Ginebra Suiza