Marco conceptual

Las tecnologías de la información y la comunicación (TIC) son el motor de la evolución de las sociedades modernas. Respaldan por igual el crecimiento social, económico y político de las personas físicas, las organizaciones y los gobiernos. Las TIC, además de ser ubicuas, son esenciales para el progreso. Los dispositivos inteligentes, las comunicaciones M2M y los servicios en la nube, entre otras muchas tecnologías, nos ayudan a avanzar hacia la próxima generación de sociedades conectadas. La tecnología digital y la conectividad a Internet están siendo integradas sistemáticamente en todos los estratos de los sectores público y privado porque ofrecen ventajas significativas: productividad, rapidez, reducción de costes y flexibilidad. En consecuencia, se están utilizando progresivamente las TIC en nuevas plataformas tales como por ejemplo sistemas RFID al detalle y telemática vehicular. Ahora bien, lo más importante es que se utilizan para mejorar infraestructuras esenciales tales como redes eléctricas, redes de transporte y sistemas de atención médica.

La ciberseguridad es fundamental para sustentar un modelo tecnológicamente coherente. Las perturbaciones del tendido eléctrico o los problemas causados a los sistemas financieros por injerencias en las redes TIC son muy concretos y constituyen amenazas para la seguridad nacional. Las personas malintencionadas en línea son numerosas, están bien organizadas y son muy diversas: políticas, delincuentes, terroristas o hacktivistas. Disponen de herramientas cada vez más sofisticadas y complejas, y adquieren experiencia con el tiempo; el número creciente de plataformas conectadas no hace más que ofrecerles nuevos vectores de ataque. Es imposible volver a los tiempos primitivos. La ciberseguridad debe formar parte integrante e indivisible del progreso tecnológico.

Lamentablemente, la ciberseguridad todavía no se considera esencial en muchas estrategias tecnológicas nacionales e industriales. Los esfuerzos para aumentar la ciberseguridad son numerosos pero eclécticos y dispersos. Las disparidades en la penetración de Internet, el desarrollo tecnológico, el dinamismo del sector privado o las estrategias públicas significan que la ciberseguridad evoluciona de lo particular a lo general, lo que es natural cuando existen esas disparidades entre Estados, sectores público y privado e incluso sectores industriales. Ahora bien, una cultura mundial de la ciberseguridad tendría más éxito en esencia si evolucionara de lo general a lo particular. La divulgación de información y la cooperación son fundamentales para afrontar las amenazas internacionales. Esos elementos requieren cierto grado de organización en numerosos ámbitos, a saber, legales, técnicos y educativos. Cuando un país determinado o

un sector específico ha desarrollado y adoptado un marco de ciberseguridad muy eficaz, pocas veces comparte ese conocimiento.

El mayor obstáculo es que la ciberseguridad es un tema delicado, ya sea para el sector público o el sector privado. Admitir vulnerabilidades puede considerarse una debilidad, y eso dificulta los debates y la divulgación de información sobre amenazas y prácticas idóneas. Ahora bien, en la seguridad, el oscurantismo no es un modelo de defensa viable contra las ciberamenazas modernas. La solución es adoptar mecanismos de ciberseguridad en todos los estratos de la sociedad. No obstante, la voluntad y los incentivos para hacerlo no son apropiados, ya sea debido a limitaciones de costes o sencillamente por falta de información. Una primera etapa para poner remedio a la situación consiste en comparar las capacidades de los países en materia de ciberseguridad y publicar la clasificación correspondiente. Esa clasificación pondría de manifiesto las deficiencias y motivaría a los Estados a intensificar sus esfuerzos de ciberseguridad. Sólo se puede evaluar realmente la capacidad de un país en materia de ciberseguridad comparándola con la de otros países.

Con el proyecto de Índice Mundial de Ciberseguridad (IMC) se intenta evaluar el grado de desarrollo de la ciberseguridad en cada país. El objetivo fundamental es fomentar la cultura mundial de la ciberseguridad y su integración en el núcleo de las tecnologías de la información y la comunicación. El proyecto ha sido lanzado por la Unión Internacional de Telecomunicaciones (UIT) y la empresa privada *ABI Research*. El proyecto se basa en el actual mandato de la UIT y los proyectos y actividades conexos de la Oficina de Desarrollo de las Telecomunicaciones (BDT) de la UIT.

La UIT es el principal facilitador en lo que respecta a la Línea de Acción C5 de la CMSI (Cumbre Mundial sobre la Sociedad de la Información), en la cual se alienta a las partes interesadas a crear confianza y seguridad en cuanto a la utilización de las TIC a escala nacional, regional e internacional. El mandato de la UIT en relación con la ciberseguridad se fundamenta además en la Resolución 69 sobre la "Creación de equipos nacionales de intervención en caso de incidente informático, especialmente para los países en desarrollo, y cooperación entre los mismos" adoptada por la quinta Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT-10), y en la Resolución 130 (Guadalajara, 2010) sobre el "Fortalecimiento del papel de la UIT en la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación". A ese respecto, el Secretario General de la UIT lanzó la Agenda sobre Ciberseguridad Global (GCA), el mecanismo de cooperación multipartita internacional creado por la UIT para orientarse hacia una sociedad de la información más segura y protegida, y que se focaliza en los cinco ámbitos de trabajo siguientes:

- Medidas legales
- Medidas técnicas
- Medidas orgánicas
- Capacitación
- Cooperación.

Estos cinco ámbitos señalados constituirán la base de los indicadores para el IMC. Son esenciales para medir las capacidades de ciberseguridad nacionales porque son los componentes inherentes de una cultura nacional. El campo de aplicación de la ciberseguridad abarca todas las industrias y todos los sectores, tanto vertical como horizontalmente. Por consiguiente, facilitar el desarrollo de capacidades nacionales exige inversiones políticas, económicas y sociales, que pueden ser obra de departamentos de policía y justicia, instituciones docentes y ministerios, operadores del sector privado y desarrolladores de tecnologías, asociaciones público-privadas y mecanismos de cooperación intraestatales.

El objetivo a largo plazo es fomentar las actividades de adopción e integración de la ciberseguridad a escala mundial. La comparación de las estrategias nacionales de ciberseguridad permitirá determinar los países que ocupan un puesto elevado en determinados ámbitos de la clasificación y, por consiguiente, dará a conocer estrategias de seguridad menos conocidas pero eficaces. De este modo se puede propiciar una mayor divulgación de información sobre la adopción de medidas de ciberseguridad entre países con niveles diferentes de desarrollo. Al medir el nivel de preparación de ciberseguridad en diversos ámbitos, el índice ayudará a los países a determinar dónde se encuentran en una escala de desarrollo, si necesitan realizar mejoras y cuánto les queda para implementar un nivel aceptable de ciberseguridad. Todos los países van camino de un entorno más digitalizado y conectado, y la pronta adopción de medidas de ciberseguridad puede ayudarles a desplegar infraestructuras más seguras y resistentes a largo plazo.

El proyecto IMC será un esfuerzo conjunto de la BDT, especialmente su división de Aplicaciones TIC y Ciberseguridad (CYB), y *ABI Research*. El Departamento CYB será el coordinador y titular del proyecto, y *ABI Research* aportará sus competencias fundamentales en materia de elaboración de estrategias, información sobre la competencia, planificación empresarial, asesoramiento tecnológico y definición de referencias de la industria para la realización del proyecto. *ABI Research* es una empresa de información sobre los mercados, especializada en los mercados mundiales de la tecnología, que realiza previsiones y análisis cuantitativos de parámetros y tendencias fundamentales. *ABI Research*, gracias a sus competencias exclusivas que le permiten facilitar perspectivas visionarias y datos utilizables, oportunos y auténticos en el sector de la tecnología, aportar sus conocimientos para el desarrollo oportuno y la producción de un índice fiable. En el marco de este acuerdo, la UIT y *ABI Research*:

- identifican unidades de medición del rendimiento;
- desarrollan un mecanismo de clasificación mundial;
- investigan y compilan datos sobre las capacidades de ciberseguridad de los países;
- establecen contactos y coordinación con Estados y organizaciones competentes;
- identifican e insertan datos pertinentes en el índice;
- publican un índice mundial de ciberseguridad.

Categorías e indicadores de rendimiento

El IMC será la referencia por la que se medirán las capacidades de desarrollo de ciberseguridad de los Estados soberanos. El índice es en esencia un indicador global que combina varios indicadores individuales. El proceso de desarrollo de la ciberseguridad se puede analizar con arreglo a cinco categorías generales importantes. Se han identificado los siguientes indicadores y subgrupos, y los países se clasifican con respecto a la referencia que constituye cada indicador.

1 Medidas legales

La legislación es esencial para crear un marco armonioso en el que las entidades se pueden adaptar a una base normativa común, ya sea con respecto a la prohibición de un determinado comportamiento delictivo, o a exigencias normativas mínimas. Con medidas legislativas los países también pueden determinar mecanismos básicos de respuesta a las infracciones, mediante investigaciones y acciones judiciales contra los delitos, y la imposición de sanciones por incumplimiento o infracción de la ley. Un marco legislativo fija las normas mínimas de comportamiento generales, aplicables para todos, y a partir de las cuales pueden crearse otras capacidades de ciberseguridad. En última instancia, el objetivo es que todos los países

dispongan de una legislación adecuada para armonizar prácticas a escala supranacional y crear un entorno propicio a la adopción de medidas compatibles, lo que facilitaría la guerra internacional contra la ciberdelincuencia.

El entorno legislativo se puede medir en función de la existencia y el número de instituciones y marcos legales que tratan de ciberseguridad y ciberdelito. El subgrupo comprende los indicadores de rendimiento siguientes:

A Legislación penal

La legislación sobre el ciberdelito contiene leyes sobre acceso no autorizado (sin derecho), interferencias, así como intercepción de computadoras, sistemas y datos. Las legislaciones se pueden clasificar por niveles: ninguna, parcial o global. La legislación parcial consiste en la simple inserción de oraciones relacionadas con la informática en una ley o un código penal existente, que se limitan a extender al ciberespacio, por ejemplo, el fraude o la falsificación, así como la vigilancia y el robo. La legislación global consiste en adoptar una ley o un código que trate de aspectos concretos del ciberdelito (por ejemplo la *Computer Misuse Act* de 1990 del Reino Unido). Esta categoría puede comprender legislaciones parciales que recurren ampliamente a la jurisprudencia. Indique los tipos de leyes y normativas, si no hay ninguna o si son parciales o globales.

B Reglamentación y conformidad

La reglamentación de la ciberseguridad consiste en leyes que tratan de protección de datos, notificación de infracciones y requisitos de certificación/normalización. Las legislaciones se pueden clasificar por niveles: ninguna, parcial o global. La reglamentación parcial consiste en insertar oraciones relacionadas con la informática en una ley o un código penal existente o nuevo, a fin de extender la aplicación de esa ley al ciberespacio en normativas que no están relacionadas específica o exclusivamente con la ciberseguridad (por ejemplo, la Directiva 95/46/CE de la UE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos). La reglamentación global consiste en promulgar un decreto, ley o directiva especial que obligue a respetar la ciberseguridad (por ejemplo la *Federal Information Security Management Act* de 2002 de Estados Unidos). Indique los tipos de leyes y normativas específicas, si no hay ninguna o si son parciales o globales.

2 Medidas técnicas

La tecnología es la primera línea de defensa contra las ciberamenazas y las personas malintencionadas en línea. Sin medidas técnicas apropiadas y las capacidades necesarias para detectar y responder a los ciberataques, los países y sus respectivas entidades son vulnerables a las ciberamenazas. Las TIC sólo se pueden afianzar, tener éxito y prosperar realmente en un clima de confianza y seguridad. Por consiguiente, los países deben poder definir estrategias para establecer criterios mínimos aceptables de seguridad y sistemas de acreditación de aplicaciones y sistemas informáticos. Estas actividades deberán acompañarse con la creación de una entidad nacional dedicada a tratar los ciberincidentes a escala nacional o, en el peor de los casos, un organismo público responsable acompañado por un marco nacional de vigilancia, aviso y respuesta en caso de incidente.

Las medidas técnicas se pueden evaluar basándose en la existencia y el número de instituciones y marcos técnicos que tratan de ciberseguridad, refrendados o creados por el Estado. El subgrupo comprende los indicadores de rendimiento siguientes:

A EIII/EIEI/EIISI

Creación de un EIII (equipo de intervención en caso de incidentes informáticos), EIEI (equipo de intervención en caso de emergencia informática) o EIISI (equipo de intervención en caso de incidente de

seguridad informática) nacional con capacidad para identificar ciberamenazas, defenderse contra ellas, responder y gestionarlas, y mejorar la seguridad del ciberespacio nacional. Ese equipo debe reunir además su propia información y no depender de información de segunda mano sobre incidentes de seguridad, ya proceda de los propios integrantes del equipo o de otras fuentes. Indique los nombres y el número de EIII o EIISI nacionales o sectoriales aprobados oficialmente, y si dispone o no de un mandato legal. El nivel de desarrollo se clasificará en función de la existencia de equipos nacionales, y de que dispongan o no de un mandato legal.

B Normas

Este indicador mide la existencia de un marco (o marcos) aprobado(s) (o refrendado(s)) por el gobierno para la aplicación de normas de ciberseguridad internacionalmente reconocidas en el sector público (organismos públicos) o en las infraestructuras esenciales (aun si son explotadas por el sector privado). Esas normas son, entre otras pero no exclusivamente, las elaboradas por los siguientes organismos: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, AIR, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc. Indique los marcos nacionales (y sectoriales) nacionales aprobados para la aplicación de normas de ciberseguridad internacionalmente reconocidas.

C Certificación

Este indicador mide la existencia de un marco (o marcos) aprobado(s) (o refrendado(s)) por el gobierno para la certificación y acreditación de organismos nacionales (gubernamentales) y profesionales del sector público con arreglo a normas de ciberseguridad internacionalmente reconocidas. Estas certificaciones, acreditaciones y normas son, entre otras pero no exclusivamente: *Cloud Security knowledge* (*Cloud Security Alliance*), CISSP, SSCP, CSSLP CBK, *Cybersecurity Forensic Analyst* (ISC²), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (*EC Council*), OSSTMM (ISECOM), PCIP/CCISP (*Critical Infrastructure Institute)*, Q/ISP, *Software Security Engineering Certification* (*Security University*), CPP, PSP, PCI (ASIS), LPQ, LPC (*Loss Prevention Institute*), CFE (*Association of Certified Fraud Examiners*), CERT-*Certified Computer Security Incident Handler* (SEI), CITRMS (*Institute of Consumer Financial Education*), CSFA (*Cybersecurity Institute*), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (*Institute of Internal Auditors*), (*Professional Risk Managers International Association*), PMP (*Project Management Institute*), etc. Indique los marcos nacionales (y sectoriales) nacionales aprobados para la certificación y acreditación de organismos nacionales y profesionales del sector público.

3 Medidas orgánicas

Para aplicar de manera adecuada cualquier tipo de iniciativa nacional se necesitan medidas de organización y procedimiento. El Estado debe fijar un objetivo estratégico general, con el correspondiente plan exhaustivo de implementación, prestación y medición. Deben crearse estructuras, tales como organismos nacionales, para llevar a efecto la estrategia y evaluar el éxito o el fracaso del plan. Sin estrategia nacional, modelo de gobernanza y organismo supervisor, los esfuerzos de los distintos sectores e industrias acaban siendo dispares e incoherentes y frustran los esfuerzos por armonizar a escala nacional el desarrollo de las capacidades de ciberseguridad.

Las estructuras orgánicas se pueden medir a partir de la existencia y el número de instituciones y estrategias que organizan el desarrollo de la ciberseguridad a escala nacional. Es necesario crear estructuras orgánicas efectivas para promover la ciberseguridad, combatir el ciberdelito y promover la importancia de la vigilancia, el aviso y la respuesta ante incidentes para garantizar la coordinación de iniciativas nuevas y existentes dentro de los organismos, entre los sectores y a través de las fronteras. El subgrupo comprende los indicadores de rendimiento siguientes:

A Política

Se reconoce que la mayor prioridad es desarrollar una política de promoción de la ciberseguridad. Una estrategia nacional de seguridad de las redes y los sistemas de información debería mantener infraestructuras de la información resistentes y fiables y tener por objeto garantizar la seguridad de los ciudadanos, proteger los activos materiales e intelectuales de los ciudadanos, organizaciones y del propio Estado, impedir ciberataques contra las infraestructuras esenciales y minimizar los daños causados por los ciberataques y el tiempo de recuperación correspondiente. Las políticas en materia de estrategias nacionales de ciberseguridad o los planes nacionales de protección de las infraestructuras de la información son los que están definidos oficialmente y refrendados por el Estado, y pueden comprender las responsabilidades siguientes: determinar claramente la responsabilidad de la ciberseguridad en todos los niveles de gobierno (local, regional y federal o nacional), con funciones y responsabilidades claramente definidas, responsabilizarse claramente de la ciberseguridad, que es pública y transparente, y fomentar la participación y asociación del sector privado en iniciativas dirigidas por el gobierno para promover la ciberseguridad. Indique las estrategias de ciberseguridad nacionales o sectoriales reconocidas oficialmente.

B Hoja de ruta para la gobernanza

Por lo general se establece una hoja de ruta para la gobernanza de la ciberseguridad por medio de una estrategia/política nacional para la ciberseguridad, en la cual se identifican los principales interesados. La elaboración de un marco de política nacional es una prioridad esencial del desarrollo de una gobernanza de alto nivel para la ciberseguridad. En ese marco de política deben tenerse en cuenta las necesidades de protección de la infraestructura nacional esencial de la información. También debe tratarse de fomentar la divulgación de información en el sector público y también entre los sectores público y privado. La gobernanza de la ciberseguridad debe fundamentarse en un marco nacional en el que se aborden las dificultades y demás cuestiones de seguridad de la información y seguridad de la red a escala nacional, a saber, entre otras, estrategia y política nacionales, fundamentos jurídicos de la transposición de leyes sobre la seguridad a entornos en red y en línea, participación de todos los interesados, desarrollo de una cultura de ciberseguridad, procedimientos para tratar las infracciones contra la seguridad de las TIC y la gestión de incidentes (informes, divulgación de información, gestión de alertas, colaboración con el poder judicial y la policía), implementación efectiva de la política nacional de ciberseguridad, control, evaluación, validación y optimización del programa de ciberseguridad. Indique las hojas de ruta nacionales o sectoriales reconocidas para la gobernanza de la ciberseguridad.

C Organismo responsable

Un organismo responsable de la implementación de una estrategia/política nacional de ciberseguridad puede estar integrado por comités permanentes, Grupos de Trabajo oficiales, consejos asesores o centros interdisciplinarios. La mayoría de los organismos nacionales serán directamente responsables de sistemas de vigilancia y alerta, y de la respuesta ante incidentes, y de la creación de las estructuras orgánicas necesarias para coordinar las respuestas a los ciberataques. Indique los organismos de ciberseguridad nacionales o sectoriales oficialmente reconocidos.

D Análisis comparativos nacionales

Este indicador mide la existencia de ejercicios de análisis comparativo nacionales o sectoriales oficialmente reconocidos, o de referencias utilizadas para medir el desarrollo de la ciberseguridad. Por ejemplo, sobre la base de la norma 27002-2005 de ISO/CEI, una norma nacional de ciberseguridad (Referencia NCSec (*National Cybersecurity Standard*)) puede ayudar a los países a responder a necesidades específicas de ciberseguridad. Esta referencia se subdivide en cinco campos: Estrategia y políticas NCSec, estructuras orgánicas NCSec, implementación de NCSec, coordinación nacional, actividades de sensibilización sobre la

ciberseguridad. Indique los ejercicios de análisis comparativo nacionales o sectoriales oficialmente reconocidos o las referencias utilizadas para medir el desarrollo de la ciberseguridad.

4 Capacitación

La capacitación forma parte integrante de las tres primeras medidas (legal, técnica y orgánica). Comprender la tecnología, sus riesgos y consecuencias puede ayudar a elaborar mejores legislaciones, políticas y estrategias, y mejorar la organización de las diversas funciones y responsabilidades. La ciberseguridad es un tema relativamente nuevo, no mucho más antiguo que la propia Internet. Es un tema que se aborda en la mayoría de los casos desde una perspectiva tecnológica pero que también tiene numerosas consecuencias socioeconómicas y políticas. La capacitación humana e institucional es necesaria para mejorar los conocimientos teóricos y prácticos en todos los sectores, aplicar las soluciones más adecuadas y promover el desarrollo de los profesionales más competentes.

El marco de capacitación para la promoción de la ciberseguridad debería comprender actividades de sensibilización y disponer de recursos. La capacitación se puede medir en función de la existencia del número de programas de investigación y desarrollo, enseñanza y capacitación, y de profesionales y organismos del sector público certificados. El subgrupo comprende los indicadores de rendimiento siguientes:

A Desarrollo de la normalización

La normalización es un buen indicador del grado de madurez de una tecnología, y la aparición de nuevas normas en ámbitos esenciales pone de manifiesto la importancia vital de las normas. Si bien la ciberseguridad siempre ha sido un asunto de seguridad nacional y se ha tratado de manera diferente en cada país, las normas comúnmente reconocidas facilitan enfoques comunes. Esas normas son, entre otras pero no exclusivamente, las elaboradas por los siguientes organismos: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, AIR, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc. Indique los programas/proyectos de investigación y desarrollo (I y D) nacionales o sectoriales oficialmente reconocidos sobre normas de ciberseguridad, prácticas idóneas y directrices que se aplicarán en el sector privado o el sector público.

B Desarrollo de la mano de obra

Para desarrollar la mano de obra los países deben esforzarse por promover campañas publicitarias generalizadas a fin de alcanzar al mayor número posible de personas, y utilizar ONG, instituciones, organizaciones, PSI, bibliotecas, organizaciones de comercio locales, centros comunitarios, tiendas informáticas, colegios comunitarios y programas de capacitación de adultos, escuelas y organizaciones de padres-maestros para informar sobre los comportamientos seguros en línea. Se trata, por ejemplo, de medidas como la creación de portales y sitios web para promover la sensibilización, la difusión de material de apoyo para educadores y el establecimiento (o la incentivación) de cursos de capacitación profesional y programas docentes. Indique los programas de capacitación educativos y profesionales nacionales o sectoriales oficialmente reconocidos destinados a aumentar la sensibilización del público en general (por ejemplo, día, semana o mes nacional de sensibilización sobre la ciberseguridad), promover cursos de ciberseguridad en la enseñanza superior (técnica, ciencias sociales, etc.) y promover la certificación de profesionales en el sector público o el sector privado.

C Certificación profesional

Este indicador de rendimiento se puede medir en función del número de profesionales del sector público certificados conforme a normas de programas de certificación internacionalmente reconocidas que son,

entre otras pero no exclusivamente: *Cloud Security knowledge* (*Cloud Security Alliance*), CISSP, SSCP, CSSLP CBK, *Cybersecurity Forensic Analyst* (ISC²), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (*EC Council*), OSSTMM (ISECOM), PCIP/CCISP (*Critical Infrastructure Institute)*, Q/ISP, *Software Security Engineering Certification* (*Security University*), CPP, PSP, PCI (ASIS), LPQ, LPC (*Loss Prevention Institute*), CFE (*Association of Certified Fraud Examiners*), CERT-*Certified Computer Security Incident Handler* (SEI), CITRMS (*Institute of Consumer Financial Education*), CSFA (*Cybersecurity Institute*), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (*Institute of Internal Auditors*), (*Professional Risk Managers International Association*), PMP (*Project Management Institute*), etc. Indique el número de profesionales del sector público certificados conforme a programas de certificación internacionalmente reconocidos.

D Certificación de organismos

Este indicador de rendimiento se puede medir en función del número de organismos gubernamentales y del sector público certificados con arreglo a normas internacionalmente reconocidas. Esas normas son, entre otras pero no exclusivamente, las elaboradas por los siguientes organismos: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, AIR, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc. Indique el número de organismos gubernamentales y del sector público certificados con arreglo a normas internacionalmente reconocidas.

5 Cooperación

La ciberseguridad necesita que todos los sectores y disciplinas contribuyan a ella y, por lo tanto, necesita un enfoque multipartito. La cooperación mejora el diálogo y la coordinación, y facilita la creación de un campo de aplicación más completo de la ciberseguridad. La divulgación de información es difícil, en el mejor de los casos, entre disciplinas diferentes y entre operadores del sector privado. Es cada vez más difícil a nivel internacional, pero el problema del ciberdelito es mundial y no conoce fronteras nacionales ni distinciones sectoriales. La cooperación facilita la divulgación de información sobre amenazas, métodos de ataque y prácticas idóneas de respuesta y defensa. Si aumentan las iniciativas de cooperación se facilitará el desarrollo de capacidades de ciberseguridad mucho mayores y, por consiguiente, se impedirán amenazas en línea reiteradas y persistentes y aumentarán las capacidades de investigación, detención y enjuiciamiento de personas malintencionadas.

La cooperación nacional e internacional se puede medir en función de la existencia y el número de asociaciones, marcos de cooperación y redes de divulgación de información. El subgrupo comprende los indicadores de rendimiento siguientes:

A Cooperación intraestatal

Cooperación intraestatal es cualquier tipo de asociación nacional o sectorial oficialmente reconocida destinada a compartir activos de ciberseguridad con otros países (es decir, asociaciones bilaterales o multilaterales de cooperación o intercambio de información, conocimientos, tecnología y/o recursos). La cooperación intraestatal también comprende iniciativas regionales tales como (pero no exclusivamente) las implementadas por la Unión Europea, el Consejo de Europa, el Grupo de Estados G8, la Cooperación Económica Asia-Pacífico (APEC), la Organización de los Estados Americanos (OEA), la Asociación de Naciones del Sudeste Asiático (ASEAN), la Liga Árabe, la Unión Africana, la *Shanghai Cooperation Organization* (SCO), grupos de operaciones de redes (*Network Operations Groups,* NOG), etc. Indique las asociaciones nacionales o sectoriales oficialmente reconocidas para compartir activos de ciberseguridad con otros países.

B Cooperación intraorganismos

Cooperación intraorganismos es cualquier programa nacional o sectorial oficialmente reconocido para compartir activos de ciberseguridad (personas, procesos, herramientas) en el sector público (es decir, asociaciones oficiales para la cooperación y el intercambio de información, conocimientos, tecnologías y/o recursos entre departamentos y organismos). Se trata de iniciativas y programas entre diversos sectores (organismos policiales, militares, salud, transporte, energía, desechos y gestión del agua, etc.) así como en departamentos/ministerios (gobiernos federales/locales, recursos humanos, servicios de asistencia informática, relaciones públicas, etc.). Indique los programas nacionales o sectoriales oficialmente reconocidos para compartir activos de ciberseguridad en el sector público.

C Asociaciones público-privadas

Las asociaciones público-privadas son asociaciones entre el sector público y el sector privado. Este indicador se puede medir en función del número de asociaciones público-privadas nacionales o sectoriales oficialmente reconocidas para compartir activos de ciberseguridad (personas, procesos, herramientas) entre el sector público y el sector privado (es decir, asociaciones oficiales para la cooperación o intercambio de información, conocimientos, tecnologías y/o recursos). Indique los programas nacionales o sectoriales oficialmente reconocidos para compartir activos de ciberseguridad entre el sector público y el sector privado.

D Cooperación internacional

Este indicador de rendimiento se refiere a cualquier participación oficialmente reconocida en plataformas y foros internacionales de ciberseguridad. Esas iniciativas de cooperación son, entre otras, pero no exclusivamente, la Asamblea General de las Naciones Unidas, la Unión Internacional de Telecomunicaciones (UIT), Interpol/Europol, la Organización de Cooperación y Desarrollo Económicos (OCDE), la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD), el Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI), la Corporación de Internet para la Asignación de Nombres y de Números (ICANN), la Organización Internacional de Normalización (ISO), la Comisión Electrotécnica Internacional (CEI), el Grupo Especial sobre Ingeniería de Internet (IETF), y el Foro de los equipos de respuesta en caso de incidentes de seguridad (FIRST). Indique las participaciones oficialmente reconocidas en plataformas y foros regionales y/o internacionales sobre ciberseguridad.

Metodología

El modelo estadístico utilizado se basará en un Análisis Multicriterios (*Multi-Criteria Analysis*, MCA), que establece preferencias entre varias opciones remitiéndose a un conjunto explícito de objetivos identificados y para las cuales existen criterios medibles establecidos destinados a evaluar hasta qué punto se han alcanzado los objetivos. Se aplicará un simple modelo lineal de evaluación por adición. En la matriz de rendimiento MCA se describen las opciones y en cada columna se indica el rendimiento de las opciones con respecto a cada criterio. La evaluación del rendimiento individual es numérica.

La puntuación se basará en los indicadores siguientes, que están ponderados cada uno por igual (aunque la ponderación de algunas subcategorías será ligeramente superior a la de otras porque algunas contienen más subgrupos). Cuando no hay actividades se da 0 puntos, 1 punto se atribuye para una acción parcial y 2 puntos para una acción más completa. El total de puntos atribuido a cada categoría es el siguiente:

1. Medidas legales	**4**
A. Legislación penal	2
B. Reglamentación y conformidad	2
2. Medidas técnicas	**6**
A. EIII/EIEI/EIISI	2
B. Normas	2
C. Certificación	2
3. Medidas orgánicas	**8**
A. Política	2
B. Hoja de ruta para la gobernanza	2
C. Organismo responsable	2
D. Análisis comparativos nacionales	2
4. Capacitación	**8**
A. Desarrollo de la normalización	2
B. Desarrollo de la mano de obra	2
C. Certificación profesional	2
D. Certificación de organismos	2
5. Cooperación	**8**
A. Cooperación intraestatal	2
B. Cooperación intraorganismos	2
C. Asociaciones público-privadas	2
D. Cooperación internacional	2

Notación:

x_{qc} Valor del indicador individual q para el país c, siendo q=1,...,Q y c=1,...,M.

I_{qc} Valor normalizado del indicador individual q para el país c

CI_c Valor del indicador compuesto para el país c

La referencia utilizada será la puntuación obtenida por el país hipotético que maximice los puntos de preparación global (34). El índice compuesto resultante irá de cero (preparación peor posible) a 1 (la referencia):

$$CI_c = \frac{I_{qc}}{34}$$

La técnica de normalización se basará en un método de clasificación:

$I_{qc} = Rank\ (x_{qc})$

La clasificación resultante se subdividirá en escalones para que los países puedan determinar los sectores que necesitan mejorar y seguir desarrollando a fin de cumplir los criterios mínimos para ascender al escalón siguiente:

Escalón 1: Alto nivel de preparación en ciberseguridad	**Mínimo 29 puntos**
Legal	Mínimo 3 puntos
Técnica	Mínimo 5 puntos
Organización	Mínimo 7 puntos
Capacitación	Mínimo 7 puntos
Cooperación	Mínimo 7 puntos
Escalón 2: Nivel intermedio de preparación en ciberseguridad	**Entre 17 y 29 puntos**
Legal	Entre 2 y 3 puntos
Técnica	Entre 3 y 5 puntos
Orgánica	Entre 4 y 7 puntos
Capacitación	Entre 4 y 7 puntos
Cooperación	Entre 4 y 7 puntos
Escalón 3: Bajo nivel de preparación en ciberseguridad	**Menos de 17 puntos**
Legal	Menos de 2 puntos
Técnica	Menos de 3 puntos
Orgánica	Menos de 4 puntos
Capacitación	Menos de 4 puntos
Cooperación	Menos de 4 puntos

Repercusiones

El objetivo a largo plazo del IMC es propiciar esfuerzos adicionales de adopción e integración de la ciberseguridad a escala mundial. La comparación entre estrategias nacionales de ciberseguridad destacará los países que ocupan un rango elevado en ámbitos específicos y, por consiguiente, sacará a la luz estrategias de ciberseguridad menos conocidas pero exitosas. De este modo se puede fomentar una mayor divulgación de información sobre el despliegue de la ciberseguridad en otros Estados que se encuentran en niveles distintos de desarrollo. Al medir el nivel de preparación de ciberseguridad en diversos ámbitos, el índice ayudará a los Estados a determinar dónde se encuentran en una escala de desarrollo, si necesitan seguir mejorando y cuánto les queda para alcanzar un nivel aceptable de ciberseguridad. Todos los Estados se orientan hacia un entorno más digitalizado y conectado, y la pronta adopción de medidas de ciberseguridad puede facilitar el despliegue de infraestructuras más seguras y resistentes.

_____