Foro Nacional de Ciberseguridad

“REPORTE CIBERSEGURIDAD 2020 RIESGOS Y AVANCES Y EL CAMINO A SEGUIR EN AMERICA LATINA Y EL CARIBE”.


D3
2016
2020
Formación, Capacitación y Habilidades de Seguridad Cibernética
3-1 Sensibilización
Programas de Sensibilización
Sensibilización Ejecutiva
3-2 Marco para la Formación
Provisión
Administración
3-3 Marco para la Capacitación Profesional
Provisión
Apropiación
D4
2016
2020
Marcos Legales y Regulatorios
4-1 Marcos Legales
Marcos Legislativos para la Seguridad de las TIC
Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
Legislación Sobre Protección de Datos
Protección Infantil en Línea
Legislación de Protección al Consumidor
Legislación de Propiedad Intelectual
Legislación Sustantiva Contra el Delito Cibernético
Legislación Procesal Contra el Delito Cibernético
4-2 Sistema de Justicia Penal
Fuerzas del Orden
Enjuiciamiento
Tribunales
4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético
Cooperación Formal
Cooperación Informal

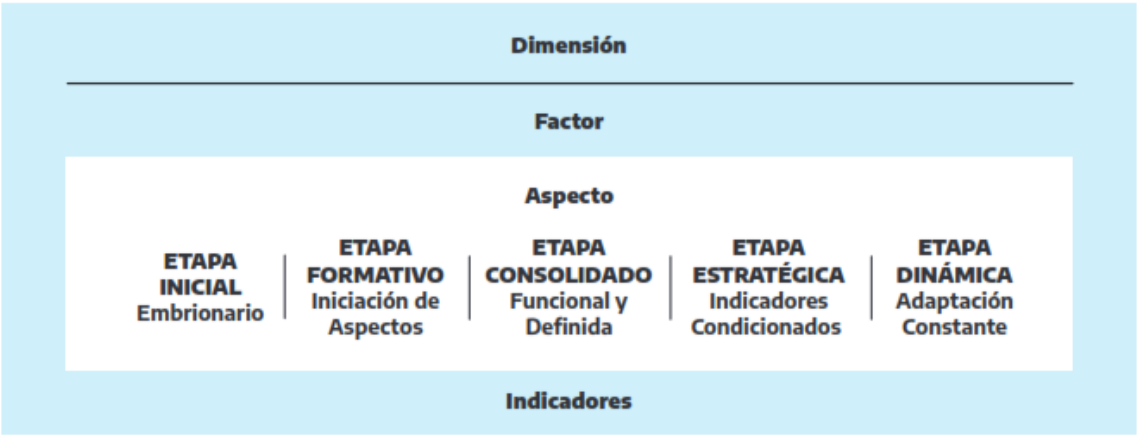

D5
2016
2020
Estándares, Organizaciones y Tecnologías
5-1 Cumplimiento de los Estándares
Estándares de Seguridad de las TIC
Estándares en Adquisiciones
Estándares en el Desarrollo de Software
5-2 Resiliencia de la Infraestructura de Internet
Resiliencia de la Infraestructura de Internet
5-3 Calidad del Software
Calidad del Software
5-4 Controles Técnicos de Seguridad
Controles Técnicos de Seguridad
5-5 Controles Criptográficos
Controles Criptográficos
5-6 Mercado de Seguridad Cibernética
Tecnologías de Seguridad Cibernética
Seguro Cibernético
5-7 Divulgación Responsable
Divulgación Responsable

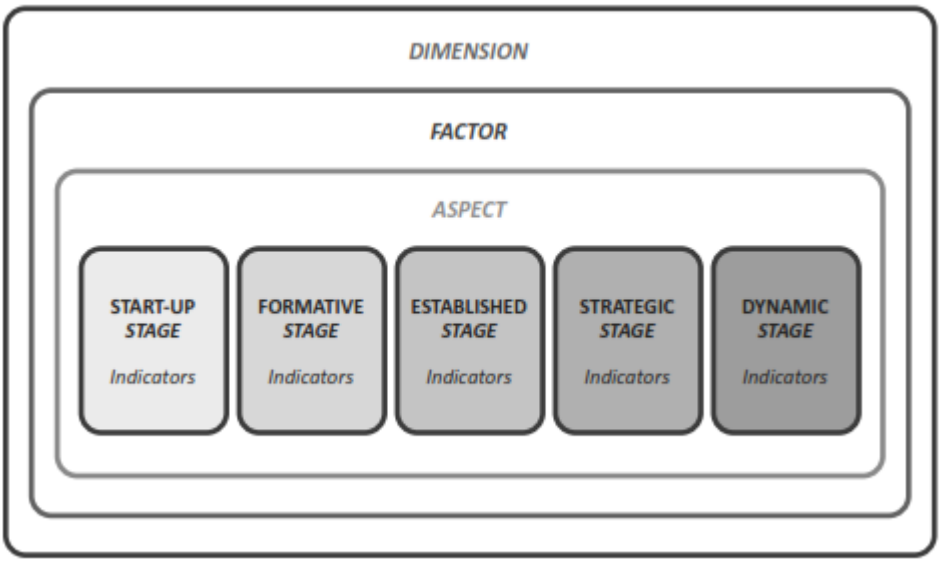
“MODELO DE MADUREZ DE CIBERCAPACIDADES PARA NACIONES (CMM) DE LA UNIVERSIDAD DE OXFORD”.

El CMM es un marco metódico diseñado por el Centro de Capacidades de Ciberseguridad Global (GCSCC, por sus siglas en inglés) de la Universidad de Oxford para evaluar la capacidad de ciberseguridad de un país como mecanismo para lograr una mejor comprensión del estado de su capacidad actual en materia de ciberseguridad y que sea de utilidad en el diseño de las políticas e iniciativas que contribuyan a incrementar su nivel de ciber-resiliencia.

La evaluación permite conocer en que etapa de madurez de ciberseguridad se encuentra un país en una escala del 1 al 5; **1** significando **etapa inicial** y **5** representando una **etapa avanzada**.

La estructura del modelo del CMM esta divido en las siguientes cuatro (4) secciones: **dimensión, factor, aspecto e indicador.**



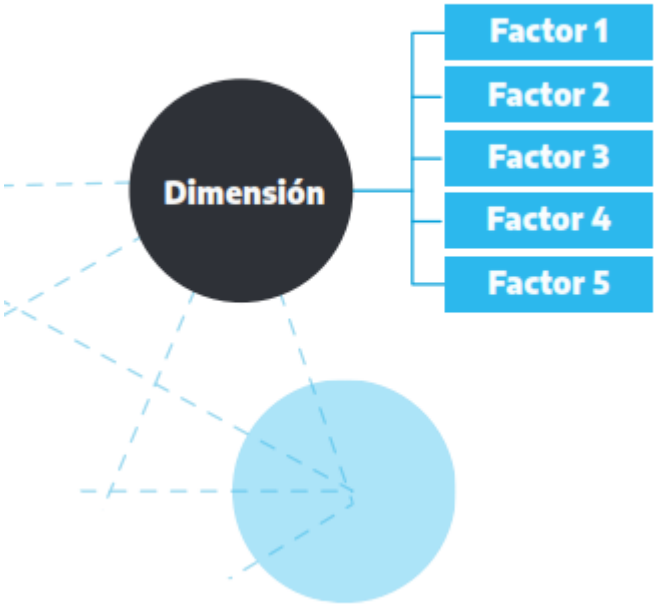


Dimensión:

Las cinco dimensiones en su conjunto cubren la amplitud de la capacidad nacional de ciberseguridad valuada por el CMM. Cada dimensión está constituida por una gama de factores, que capturan las capacidades básicas requeridas para informar la dimensión, en conjunto representan las diferentes perspectivas a través de las cuales se puede evidenciar y analizar la capacidad de ciberseguridad. El CMM considera cinco dimensiones que en su conjunto constituyen la amplitud de la capacidad nacional que un país requiere para integrar la ciberseguridad a nivel nacional:

Factores:

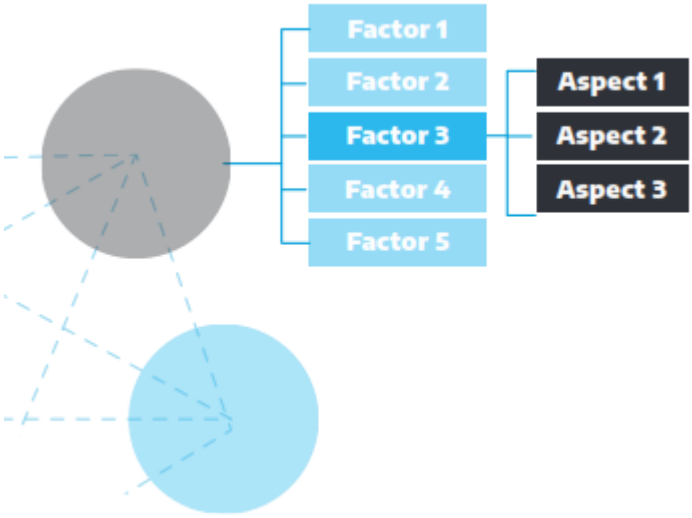
Dentro de las cinco dimensiones, los factores describen lo que significa poseer capacidad de ciberseguridad. Estos son los elementos esenciales de la capacidad nacional, que luego se miden para la etapa de madurez. La lista completa de factores busca incorporar todas las necesidades de capacidad de ciberseguridad de una nación. La mayoría de los factores se componen de una serie de aspectos que estructuran los indicadores del factor en partes más concisas (que se relacionan directamente con la recopilación y medición de evidencia). Sin embargo, algunos factores que tienen un alcance más limitado no tienen aspectos específicos.



Aspecto:

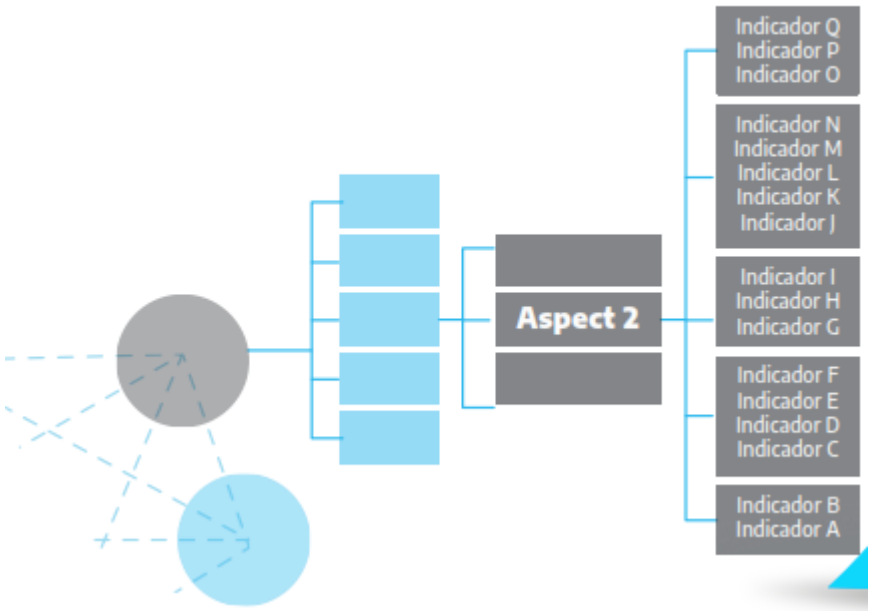
Cuando un factor posee múltiples componentes, estos son aspectos. Los aspectos son un método organizativo para dividir los indicadores en grupos más pequeños que son más fáciles de comprender.

El número de aspectos depende de los temas que surgen en el contenido del factor y la complejidad general de este.



Indicador:

Los indicadores representan la parte más básica de la estructura de CMM. Cada indicador describe los pasos, acciones o componentes básicos que son indicativos de una etapa específica de madurez. Para haber alcanzado con éxito una etapa de madurez, un país necesita evidenciar cada uno de los indicadores y para elevar la madurez de la capacidad de ciberseguridad de un país, se deberán haber cumplido todos los indicadores dentro de una etapa en particular.



Dimensión 1: Política y Estrategia Nacional de Ciberseguridad

La primera dimensión explora la capacidad del país para desarrollar y publicar una estrategia nacional de ciberseguridad, así como mejorar su resiliencia en ciberseguridad a través de la mejora de su respuesta a incidentes, ciberdefensa y capacidades de protección de infraestructura crítica. De igual manera, la presente dimensión considera la efectividad de la estrategia y política para brindar capacidad nacional de ciberseguridad, mientras se mantienen los beneficios de un ciberespacio vital para el gobierno, las empresas internacionales y la sociedad en general.

Factor D 1.1: Estrategia Nacional de Ciberseguridad

La estrategia de ciberseguridad es esencial para la transversalización de una agenda de ciberseguridad en todo el gobierno, dado que contribuye a priorizar la ciberseguridad como un área de política clave, determina responsabilidades y mandatos de actores gubernamentales claves en materia de ciberseguridad, y determina la asignación de recursos para problemas emergentes, existentes y prioridades en ciberseguridad.

Aspectos

- **Desarrollo de la Estrategia:** este aspecto aborda el desarrollo de una estrategia nacional, la asignación de autoridades de implementación entre los sectores y la sociedad civil, y una comprensión de los riesgos y amenazas de la ciberseguridad nacional que impulsan el desarrollo de capacidades a nivel nacional.
- **Contenido:** este aspecto aborda el contenido de la estrategia nacional de ciberseguridad y si está vinculada explícitamente a los riesgos, prioridades y objetivos nacionales tales como seguridad nacional, concientización pública y mitigación del ciberdelito, capacidad de respuesta a incidentes y protección de la infraestructura crítica a nivel nacional.
- **Implementación y Revisión:** este aspecto aborda la existencia de un programa integral para la coordinación de la ciberseguridad, incluyendo un propietario departamental o un organismo coordinador con un presupuesto consolidado.
- **Compromiso Internacional:** este aspecto explora el alcance de concientización del país sobre la existencia de discusiones y debates internacionales relacionadas con la política de ciberseguridad y temas relacionados que afectan los intereses del país y su postura internacional.

Factor D 1.2: Respuesta a Incidentes y Gestión de Crisis

Este factor aborda la capacidad del gobierno para identificar y determinar las características de los incidentes a nivel nacional de manera sistemática. Igualmente revisa la capacidad del gobierno para organizar, coordinar y operacionalizar la respuesta a incidentes, y si la ciberseguridad se ha integrado en el marco nacional de gestión de crisis.

Aspectos

- **Identificación y Categorización de Incidentes:** este aspecto identifica si existen mecanismos internos para identificar y categorizar incidentes.
- **Organización:** este aspecto aborda la existencia de un organismo central designado para recopilar información sobre incidentes y su relación con el sector público y privado para la respuesta a incidentes a nivel nacional.
- **Integración Cibernética en la Gestión Nacional de Crisis:** este aspecto explora el alcance en el que la ciberseguridad está integrada en el marco nacional de gestión de crisis.

Factor D 1.3: Protección de Infraestructura Crítica (IC)

Este factor estudia la capacidad del gobierno para identificar activos de IC, los requisitos regulatorios específicos de ciberseguridad de la IC y la implementación de buenas prácticas en materia de ciberseguridad por parte de los operadores de IC.

Aspectos

- **Identificación:** este aspecto aborda la existencia de una lista general de activos, sectores y operadores de IC, y una auditoría de los activos de IC de forma periódica;

- **Requisitos regulatorios:** este Aspecto aborda la existencia de requisitos regulatorios específicos para la ciberseguridad de la IC.
- **Práctica operativa:** este aspecto explora si los operadores IC implementan estándares reconocidos de la industria, y la existencia de acuerdos de colaboración entre sectores y dentro de los sectores.

Factor D 1.4: Ciberseguridad en defensa y seguridad nacional

Este factor explora si el gobierno tiene la capacidad de diseñar e implementar una estrategia de ciberseguridad dentro de la seguridad y defensa nacional. También revisa el nivel de capacidad de ciberseguridad dentro de la seguridad nacional y establecimiento de defensa, y los acuerdos de colaboración en ciberseguridad entre entidades civiles y de defensa.

Aspectos

- **Estrategia de ciberseguridad de la fuerza de defensa:** este aspecto aborda la existencia de una estrategia de apoyo hacia la ciberseguridad dentro de la seguridad nacional y la defensa, y si está respaldado por las autoridades legales apropiadas y doctrina operativa relevante y reglas de compromiso;
- **Capacidad de ciberseguridad de la fuerza de defensa:** este aspecto revisa el nivel de capacidad de ciberseguridad y estructuras organizativas dentro de la seguridad nacional establecida;
- **Coordinación de la defensa civil:** este aspecto examina la colaboración en ciberseguridad entre entidades civiles y de defensa, y la existencia de recursos adecuados establecidos.

Dimensión 2: Cultura y Sociedad Cibernética

La segunda dimensión revisa elementos importantes sobre la adquisición de una cultura de ciberseguridad responsable, como la comprensión de los riesgos relacionados con la ciberseguridad en la sociedad, el nivel de confianza en los servicios de Internet, los servicios de gobierno electrónico y de comercio electrónico, y la comprensión de los usuarios sobre la protección de la información personal en línea. Esta dimensión explora la existencia de mecanismos de denuncia que funcionan como canales para que los usuarios informen el ciberdelito. Adicionalmente, la revisión del rol de los medios de comunicación y las redes sociales en inducir valores, actitudes y comportamiento en ciberseguridad es contemplado dentro de dicha dimensión.

Factor 2.1: Mentalidad de ciberseguridad

Este factor evalúa el grado en que la ciberseguridad se prioriza e incorpora en los valores, actitudes y prácticas del gobierno, el sector privado y los usuarios en toda la sociedad. Una mentalidad de ciberseguridad consiste en valores, actitudes y prácticas, incluidos los hábitos de usuarios individuales, expertos y otros actores, en el ecosistema de ciberseguridad que aumentan la capacidad de los usuarios para protegerse asimismo en línea.

Aspectos

- **Conciencia de los riesgos:** este aspecto examina el nivel de conciencia de los riesgos de ciberseguridad dentro del gobierno, sector privado y usuarios;
- **Prioridad de seguridad:** este aspecto examina el grado de prioridad que el gobierno, el sector privado y los usuarios le dan a la ciberseguridad; y
- **Prácticas:** este aspecto examina si el gobierno, el sector privado y los usuarios siguen prácticas seguras de ciberseguridad.

Factor D 2.2: Confianza y seguridad en los servicios en línea

Este factor revisa las habilidades críticas, la administración de la desinformación, el nivel de confianza y seguridad de los usuarios en el uso de los servicios en línea en general y en particular, del gobierno electrónico y servicios de comercio electrónico.

Aspectos

- **Capacitación y habilidades digitales:** este aspecto examina si los usuarios de Internet evalúan críticamente lo que ven o reciben en línea;
- **Seguridad y Confianza del usuario en la búsqueda en línea e información:** este aspecto examina si los usuarios confían en el uso seguro de Internet basado en indicadores de la legitimidad del sitio web;
- **Desinformación:** este aspecto examina la existencia de herramientas y recursos para abordar la desinformación en línea;
- **Confianza del usuario en los servicios de gobierno electrónico:** este aspecto examina si se ofrecen servicios electrónicos gubernamentales, si existe confianza en la provisión segura de tales servicios, y si se realizan esfuerzos para promover dicha confianza en la aplicación de medidas de seguridad;
- **Confianza del usuario en los servicios de comercio electrónico:** este aspecto examina si los servicios de comercio electrónico se ofrecen y se establecen en un entorno seguro y de confianza para los usuarios.

Factor 2.3: Comprensión del usuario de la protección en línea de la información personal

Este factor analiza si los usuarios de Internet y las partes interesadas dentro del sector público y privado reconocen y comprenden la importancia de proteger información personal en línea, y si son conscientes de sus derechos de privacidad.

Aspectos

- **Protección de información personal en línea:** analiza si los usuarios de Internet y las partes interesadas dentro del sector público y privado reconocen y comprenden la importancia de proteger información personal en línea, y si son conscientes de sus derechos de privacidad.

Factor D 2.4: Mecanismos de notificación

Este factor explora la existencia de mecanismos de denuncia que funcionan como canales para que los usuarios denuncien delitos relacionados con Internet tales como fraude en línea, acoso cibernético, abuso infantil en línea, robo de identidad, violaciones a la privacidad y la seguridad, y otros incidentes.

Aspectos

- **Mecanismos de notificación:** explora la existencia de mecanismos de denuncia que funcionan como canales para que los usuarios denuncien delitos relacionados con Internet tales como fraude en línea, acoso cibernético, abuso infantil en línea, robo de identidad, violaciones a la privacidad y la seguridad, y otros incidentes.

Factor D 2.5: Plataformas en línea y medios de comunicación

Este factor explora si la ciberseguridad es un tema común de discusión en los principales medios de comunicación, y un tema para una amplia discusión en las redes sociales. Además, este factor analiza el papel de los medios de comunicación en la transmisión al público de información sobre ciberseguridad, dando forma a sus valores y actitudes de ciberseguridad y comportamiento en línea.

Aspectos:

- **Medios de comunicación y redes sociales:** explora si la ciberseguridad es un tema común de discusión en los principales medios de comunicación, y un tema para una amplia discusión en las redes sociales. Además, se analiza el papel de los medios de comunicación en la transmisión al público de información sobre ciberseguridad, dando forma a sus valores y actitudes de ciberseguridad y comportamiento en línea.

Dimensión 3: Desarrollando Conocimiento y Capacidades en Ciberseguridad

La tercera dimensión revisa la disponibilidad, calidad y aceptación de programas para varios grupos de partes interesadas, incluido el gobierno, el sector privado y la población en general, y se relaciona con programas de concienciación sobre ciberseguridad, programas oficiales educativos en ciberseguridad, así como programas de formación profesional.

Factor 3.1: Desarrollo de Concientización en Ciberseguridad

Este factor se centra en la disponibilidad de programas que crean conciencia sobre la ciberseguridad en todo el país, concentrándose en los riesgos y amenazas de ciberseguridad y las formas para abordarlos.

Aspectos

- **Iniciativas gubernamentales de sensibilización:** este aspecto examina la existencia de un programa coordinado a nivel nacional de sensibilización en ciberseguridad impulsado por el

gobierno, cubriendo una amplia gama de datos demográficos y cuestiones, desarrolladas en consulta con las partes interesadas de varios sectores;

- **Iniciativas de sensibilización del sector privado:** este aspecto examina la existencia de programas de sensibilización impulsados por el sector privado y la medida en que son alineados con iniciativas gubernamentales y de la sociedad civil;
- **Iniciativas de sensibilización de la sociedad civil:** este aspecto examina la existencia de programas de sensibilización impulsados por la sociedad civil y el grado en que son alineados con iniciativas gubernamentales y del sector privado; y
- **Sensibilización ejecutiva:** este aspecto examina los esfuerzos para sensibilizar a los ejecutivos sobre los problemas de ciberseguridad en los sectores público, privado, académico y de la sociedad civil, además de cómo se pueden abordar los riesgos de ciberseguridad.

Factor D 3.2: Educación en ciberseguridad

Este factor aborda la disponibilidad y provisión de programas de educación en ciberseguridad de alta calidad y suficientes profesores e instructores cualificados. Adicionalmente, este factor examina la necesidad de mejorar la educación en ciberseguridad a nivel nacional e institucional y la colaboración entre el gobierno y la industria para asegurar que las inversiones educativas satisfagan las necesidades del entorno educativo en ciberseguridad en todos los sectores.

Aspectos

- **Provisión:** este aspecto explora si existen ofertas de programas de alta calidad en ciberseguridad y suficientes profesores cualificados disponibles que brindan una comprensión de los riesgos actuales y los requisitos de las habilidades; y
- **Administración:** este aspecto explora la coordinación y recursos para desarrollar y mejorar los marcos educativos en ciberseguridad con presupuesto y gastos asignados basados en la demanda nacional.

Factor D 3.3: Formación profesional en ciberseguridad

Este factor aborda y revisa la disponibilidad y provisión de programas asequibles de formación profesional en ciberseguridad para construir un organismo de profesionales de ciberseguridad. Además, este factor revisa la adopción de la formación horizontal y vertical del conocimiento en ciberseguridad y la transferencia de habilidades dentro de las organizaciones, y cómo esta transferencia de habilidades se traduce en un aumento continuo de organismos de profesionales de ciberseguridad.

Aspectos

- **Provisión:** este aspecto examina el desarrollo, disponibilidad y provisión de programas de capacitación en ciberseguridad para mejorar habilidades y capacidades;
- **Admisión:** este aspecto examina la aceptación y la disponibilidad de tales programas para producir un organismo de profesionales certificados en ciberseguridad. Los problemas

investigados incluyen iniciativas para registrarse en dichos programas, iniciativas para permanecer en el país después de completar con éxito, compartir conocimientos después de completar un programa, y la existencia de un registro nacional de estudiantes exitosos y certificados.

Factor D 3.4: Investigación e innovación en ciberseguridad

Este factor aborda el énfasis puesto en la investigación sobre ciberseguridad e innovación para abordar los retos tecnológicos, sociales y empresariales y avanzar en la construcción de conocimientos y capacidades de ciberseguridad en el país.

Aspectos

- Investigación y desarrollo en ciberseguridad: este aspecto investiga la existencia de una cultura de investigación e innovación en el país, relacionado con proyectos nacionales actuales y terminados, apoyo financiero, incentivos y resultados de investigación utilizables.

Dimensión 4: Marcos Legales y Regulatorios

Esta dimensión examina la capacidad del gobierno para diseñar y promulgar legislación nacional que se relacione directa e indirectamente con la ciberseguridad, con un énfasis particular en los temas de los requisitos regulatorios para la ciberseguridad, la legislación relacionada con el delito cibernético y la legislación relacionada. La capacidad para hacer cumplir tales leyes se examina a través de la aplicación de la ley, el enjuiciamiento, los órganos reguladores y los tribunales. Además, esta dimensión observa cuestiones como los marcos de cooperación formales e informales para combatir el ciberdelito.

Factor D 4.1: Disposiciones legales y regulatorias

Este factor aborda diversas leyes y provisiones de regulación relativas a la ciberseguridad, incluidos los requisitos legales y regulatorios, legislación sustantiva y procesal sobre ciberdelincuencia e impacto y evaluación sobre los derechos humanos.

Aspectos

- **Legislación sustantiva sobre ciberdelincuencia:** este aspecto explora si la legislación existente penaliza una variedad de delitos cibernéticos en legislación específica o derecho penal general;
- **Requisitos legales y regulatorios para la ciberseguridad:** este aspecto revisa la existencia de marcos legales y regulatorios en ciberseguridad;
- **Legislación procesal sobre ciberdelincuencia:** este aspecto examina si es implementado el derecho procesal penal integral con poderes procesales para la investigación del delito cibernético y requisitos probatorios para disuadir, responder y enjuiciar el ciberdelito y los delitos que involucran evidencia electrónica, y

- **Evaluación de impacto en derechos humanos:** este aspecto examina si se llevan a cabo las evaluaciones de impacto sobre si la legislación procesal sobre ciberdelincuencia y las regulaciones de ciberseguridad cumplen con los estándares internacionales de protección de derechos humanos y otros derechos fundamentales.

Factor D 4.2: Marcos legislativos relacionados

Este factor aborda los marcos legislativos relacionados con ciberseguridad, incluida la protección de datos, protección infantil, protección del consumidor y propiedad intelectual.

Aspectos

- **Legislación de protección de datos:** este aspecto examina la existencia e implementación de un marco legal para asegurar la protección de datos;
- **Protección infantil en línea:** este aspecto se centra en el marco legal para asegurar la protección de niños y niñas en línea, incluida la protección de sus derechos en línea y la criminalización de abuso infantil en línea;
- **Legislación de Protección al Consumidor:** este aspecto aborda la existencia y aplicación de la legislación que protege consumidores en línea del fraude y otras formas de negligencia empresarial;
- **Legislación de Propiedad Intelectual:** este aspecto está relacionado con la existencia e implementación de la legislación de propiedad intelectual en línea.

Factor D 4.3. Capacidad y habilidad legal y regulatoria

Este factor estudia la capacidad de aplicar la ley para investigar el delito cibernético, la capacidad de la fiscalía para presentar casos de ciberdelincuencia y pruebas electrónicas, y capacidad del tribunal para presidir casos de ciberdelincuencia y que involucre evidencia electrónica. Finalmente, este factor revisa la existencia de organismos reguladores intersectoriales para supervisar el cumplimiento de normativas específicas de ciberseguridad.

Aspectos

- **Aplicación de la ley:** este aspecto examina si los agentes y organismos encargados de hacer cumplir la ley han recibido la formación en la investigación y gestión de casos de ciberdelincuencia, y casos de delitos informáticos que involucran evidencia electrónica, y si hay suficientes recursos humanos, procedimentales y tecnológicos;
- **Enjuiciamiento:** este aspecto examina si los fiscales han recibido formación sobre el manejo de casos de ciberdelincuencia y casos que involucran evidencia electrónica, y si hay suficientes recursos humanos, procedimentales y tecnológicos;
- **Tribunales:** este aspecto examina si los tribunales tienen suficientes recursos y formación para garantizar un enjuiciamiento efectivo y eficiente de casos de ciberdelincuencia y casos que involucren evidencia electrónica;

- **Órganos reguladores:** este aspecto revisa la existencia de organismos reguladores intersectoriales para supervisar el cumplimiento de normativas específicas de ciberseguridad.

Factor D 4.4: Marcos de Cooperación formal e informal para combatir la ciberdelincuencia

Este factor aborda la existencia y función de los mecanismos formales e informales que permitan la cooperación entre actores nacionales y transfronterizos para disuadir y combatir ciberdelito.

Aspectos

- **Cooperación de la aplicación de la ley con el sector privado:** este aspecto examina el mecanismo de intercambio de información sobre la ciberdelincuencia entre los sectores público y privado nacional, incluida la cooperación con el servicio de Internet y otros proveedores de tecnología;
- **Cooperación con homólogos extranjeros encargados de hacer cumplir la ley:** este aspecto examina la existencia de mecanismos formales de cooperación internacional en materia de aplicación de la ley;
- **Colaboración entre el gobierno y el sector de la justicia penal:** este aspecto revisa los canales formales de comunicación entre el gobierno y los actores de la justicia penal.

Dimensión 5: Estándares y Tecnologías

Esta dimensión aborda el uso de tecnología en ciberseguridad de forma eficaz y difusiva para proteger individuos, organizaciones e infraestructura nacional. La dimensión examina específicamente la implementación de estándares y buenas prácticas en materia de ciberseguridad, la ejecución de procesos y controles, además del desarrollo de tecnologías y productos para reducir los riesgos asociados a la ciberseguridad.

Pruebas de conceptos y prototipos de política pública aborda aquellas iniciativas sobre materias específicas o propias que se consideren relevantes y sobre las cuales es importante formar opinión.

Factor D 5.1: Cumplimiento de los estándares

Este factor revisa la capacidad del gobierno para promover, evaluar, implementar y monitorear el cumplimiento de estándares y buenas prácticas internacionales de ciberseguridad.

Aspectos

- Estándares de seguridad ICT: este aspecto examina si los estándares y buenas prácticas internacionales relacionadas con la ciberseguridad se adoptan e implementan ampliamente en todo el sector público y organizaciones de infraestructura critica;
- Estándares en Adquisiciones: este aspecto aborda la implementación de estándares y buenas prácticas en todos los sectores para orientar los procesos de adquisiciones, incluido el riesgo de gestión, gestión del ciclo de vida, aseguramiento de software y hardware, subcontratación y uso de servicios en la nube;

- Estándares para la provisión de productos y servicios: este aspecto aborda el uso de estándares y buenas prácticas por proveedores locales de bienes y servicios, incluyendo software, hardware, servicios gestionados y servicios en la nube.

Factor D 5.2: Controles de seguridad

Este factor revisa la evidencia con respecto al despliegue de controles de seguridad por parte de usuarios y sectores público y privado, y si el conjunto de control de ciberseguridad tecnológica es basado en marcos de ciberseguridad establecidos.

Aspectos

- Controles de seguridad tecnológica: este aspecto explora en qué medida los controles de seguridad tecnológicos actualizados, incluidos parches y copias de seguridad, se implementan en todos los sectores.
- Controles criptográficos: este aspecto revisa el despliegue de técnicas criptográficas en todos los sectores y usuarios para protección de datos en reposo o en tránsito, y el grado en que estos controles criptográficos cumplen con normas y directrices internacionales y se mantienen actualizadas.

Factor D 5.3: Calidad del software

Este factor examina la calidad de la implementación de software y los requisitos funcionales en los sectores público y privado. Además, este factor revisa la existencia y mejora de políticas y procesos para actualizaciones de software y mantenimiento basado en evaluaciones de riesgo y la naturaleza crítica de los servicios.

Aspectos

- Calidad y garantía del software: examina la calidad de la implementación de software y los requisitos funcionales en los sectores público y privado. Además, se revisa la existencia y mejora de políticas y procesos para actualizaciones de software y mantenimiento basado en evaluaciones de riesgo y la naturaleza crítica de los servicios.

Factor D 5.4: Comunicaciones e Internet Resiliencia de la infraestructura

Este factor aborda la existencia de infraestructura y servicios de Internet confiables en el país, así como procesos de seguridad rigurosos en los sectores público y privado. Además, este factor revisa el control que el gobierno podría tener sobre su infraestructura de Internet y la medida en que se subcontratan las redes y los sistemas.

Aspectos

- **Confiabilidad de la Infraestructura de Internet: este** Aspecto examina la confiabilidad y protección de los servicios e infraestructura de Internet en los sectores público y privado; y
- **Monitoreo y respuesta:** este aspecto examina si existen mecanismos para realizar evaluaciones de riesgo y monitorear la resiliencia de la red en los sectores público y privado.

Factor D 5.5: Mercado de ciberseguridad

Este factor aborda la disponibilidad y el desarrollo de tecnologías de ciberseguridad competitivas, productos de ciberseguros, servicios y experiencia en ciberseguridad, y las implicaciones de seguridad de la subcontratación.

Aspectos

- Tecnologías de ciberseguridad: este aspecto examina si existe un mercado nacional para tecnologías de ciberseguridad y si está respaldado e informado por la demanda nacional;
- Servicios y experiencia en ciberseguridad: este aspecto explora la disponibilidad de servicios de consultoría en ciberseguridad para organizaciones públicas y privadas;
- Implicaciones de seguridad de la subcontratación: este aspecto examina si se realizan evaluaciones de riesgo para determinar cómo mitigar los riesgos de subcontratar TI a un tercero o servicios en la nube; y
- Seguros de ciberseguridad: este aspecto explora la existencia de un mercado de seguros cibernéticos, su cobertura y productos adecuados para diversas organizaciones.

Factor D 5.6: Divulgación responsable

Este factor explora el establecimiento de un marco de divulgación responsable para la recepción y difusión de información de vulnerabilidad en todos los sectores, y si existe la capacidad suficiente para revisar y actualizar continuamente este marco.

Aspectos

- **Compartir información sobre vulnerabilidades:** este aspecto explora los mecanismos o canales existentes para compartir información sobre los detalles técnicos de las vulnerabilidades entre las partes interesadas; y
- **Políticas, Procesos y Legislación para la divulgación responsable de fallas de seguridad:** este aspecto explora la existencia de una política o marco de divulgación responsable en organizaciones del sector público y privado y el derecho a la protección legal para quienes divulgan fallas de seguridad.