EL BANCO MUNDIAL
BIRF • AIF

DIAGNÓSTICO DE LAS CAPACIDADES DE CIBERSEGURIDAD

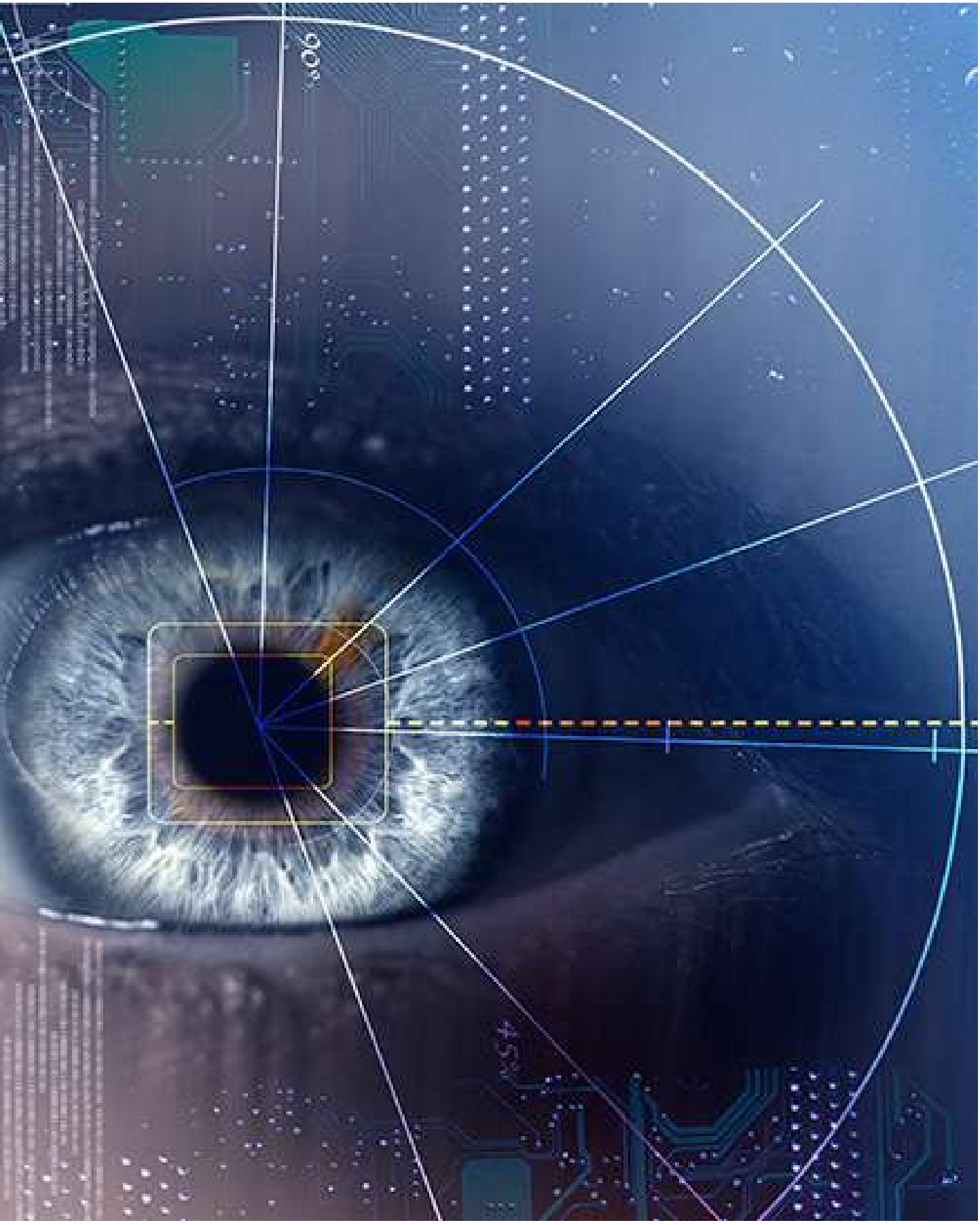
ECUADOR
DICIEMBRE 2022

Ministerio de Telecomunicaciones y de la Sociedad de la Información

República del Ecuador

Descargo de responsabilidad

Para la elaboración del presente diagnóstico, el equipo de investigación organizó varios grupos de trabajo y recopiló información hasta el mes de marzo del 2022, por lo que cualquier avance o mejora en las capacidades de ciberseguridad de Ecuador que sea posterior a esa fecha, no forma parte del presente diagnóstico. Sin embargo, a petición de MINTEL, el equipo de investigación realizó una actualización parcial, puntualmente en los factores D1.1, D4.1, y D4.3. Solo en D1.1 se modificó el nivel de madurez alcanzado inicialmente. Esas actualizaciones constan en tres cuadros debidamente identificados, en los cuales se describen tres logros importantes que Ecuador alcanzó recientemente en el ámbito de la ciberseguridad.



Conteni

do

ADMINISTRACIÓN DE DOCUMENTO

Consultor e Investigador Líder:	Óscar Noé Ávila (Banco Mundial)
Proyecto Liderado por:	Axel Rifon Pérez (Banco Mundial)
Revisado por:	Giacomo Assenza (Banco Mundial)
Editado por:	Marisol Ruelas (Banco Mundial)
Con el apoyo de:	Polo Fabián Íñiguez Matute (Subsecretario de Gobierno Electrónico y Registro Civil, MINTEL)

Versión	Fecha	Notas
vo1	27-04-2022	Primer borrador presentado a MINTEL
vo2	10-08-2022	Segundo borrador presentado a MINTEL
vo2	10-08-2022	Aprobado por MINTEL y Solicitud de Actualización
vo3	19-09-2022	Tercer borrador presentado a MINTEL
vo3	29-09-2022	Aprobado por MINTEL
vo4	19-10-2022	Borrador Final
vo5	12-12-2022	Edición y revisión interna por parte del Banco Mundial
Vo6	16-12-2022	Versión Final

EL BANCO MUNDIAL
BIRF • AIF

LISTA DE SIGLAS

ACI	Airports Council Internacional
ACI-LAC	Oficina Regional del ACI
AECI	Asociación Ecuatoriana de Ciberseguridad
ALC	América Latina y el Caribe
ARCOTEL	Agencia de Regulación y Control de las Telecomunicaciones
BID	Banco Interamericano de Desarrollo
CECE	Cámara Ecuatoriana de Comercio Electrónico
CEDIA	Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia
CELEC	Corporación Eléctrica del Ecuador
CERT	Computer Emergency Response Team
CIES	Centro de Inteligencia Estratégica
CISA	ISACA Certified Information System Auditor
CISO	Chief Information Security Officer
CMM	Cybersecurity Capacity Maturity Model for Nations
CNC	Comité Nacional de Ciberseguridad
CNE	Consejo Nacional Electoral
CNT	Corporación Nacional de Telecomunicaciones
COBIT	Control Objectives for Information and Related Technologies
COCIBER	Comando de Ciberdefensa
COIP	Código Orgánico Integral Penal
CPCCS	Consejo de Participación Ciudadana y Control Social
CPS	Sistema ciberfísico dotado por la Embajada de Gran Bretaña, para la lucha de delitos informáticos.
Cyber4Dev	EU Cyber Resilience for Development- European Union funded project
CyberNet	EU CyberNet, a European Union-funded project
DAC	Dirección de Aviación Civil
DDoS	Distributed Denial of Services
DIGERCIC	Dirección General del Registro Civil, Identificación y Cedulación
DINARP	Dirección Nacional de Registros Públicos
ECUCERT	Centro de Respuesta a Incidentes Informáticos del Ecuador
EGSI Ver. 2.0	Esquema Gubernamental de Seguridad de la Información Versión 2
ESPOL	Escuela Superior Politécnica del Litoral
FIC	Foro Interamericano de Ciberdefensa
GCSCC	Global Cybersecurity Capacity Centre
IGF	Internet Governance Forum
IRCA	International Register of Certified Auditors
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
LOPDP	Ley Orgánica de Protección de Datos Personales
MDN	Ministerio de Defensa Nacional
MINTEL	Ministerio de Telecomunicaciones y de la Sociedad de la Información
MITRE	MITRE Corporation
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OCDE	Organización para la Cooperación y el Desarrollo Económico
OEA	Organización de los Estados Americanos
ONG	Organización No-Gubernamental
OSINT	Open-Source intelligence
OT	Operational Technology
OWASP	Open Web Application Security Project
PAcCTO	Pacto de Asistencia contra el Crimen Transnacional Organizado
PDN	Política de Defensa Nacional del 2018
PNC	Política Nacional de Ciberseguridad
PYMES	Pequeñas y Medianas Empresas
PUCE	Pontificia Universidad Católica del Ecuador
RNC	Red Nacional de Confianza
SERCOP	Servicio Nacional de Contratación Pública
SOC	Security Operations Center
SPD	Superintendencia de Protección de Datos (pendiente de creación)
SNRE	Servicio Nacional de Riesgos y Emergencia
TIC	Tecnologías de la Información y la Comunicación
TLS	Transport Layer Security
UCE	Universidad Central del Ecuador
UDLA	Universidad de las Américas
UIDE	Universidad Internacional del Ecuador
UIT	Unión Internacional de Telecomunicaciones
UISEK	Universidad Internacional SEK
UNIR	Universidad Internacional de La Rioja
UTEG	Universidad Tecnológica Empresarial de Guayaquil
UTN	Universidad Técnica del Norte
VPN	Virtual Private Network
WEBINT	Web Intelligence
WIPO	World Intellectual Property Organization

RESUMEN EJECUTIVO

1. Por invitación del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) y del Comité Nacional de Ciberseguridad, el Banco Mundial llevó a cabo un diagnóstico para determinar el nivel madurez de las capacidades de ciberseguridad en la República del Ecuador. El objetivo de este diagnóstico es permitir que el país tenga a su disposición un estudio que permita una mejor comprensión de sus capacidades de ciberseguridad para priorizar estratégicamente tanto la revisión/actualización de la actual Política Nacional de Ciberseguridad y desarrollado de la Estrategia Nacional de Ciberseguridad (Plan de Acción) como la inversión en ciberseguridad, específicamente en aquellos temas que son prioritarios a nivel nacional.

2. Durante el período de diciembre de 2021 a enero del 2022, las siguientes partes interesadas participaron en reuniones presenciales y virtuales: representantes de la academia, de agencias de cumplimiento de la ley, de la Fiscalía General del Estado, de la Corte Nacional de Justicia, de entidades del sector público, de infraestructuras críticas, de instituciones a cargo de formular políticas públicas, del sector de tecnología de la información del gobierno y el sector privado (incluidas las instituciones financieras), de los centros de respuesta a incidentes cibernéticos del sector público y privado, del sector privado en general, de la sociedad civil, del sector de telecomunicaciones, del sector financiero, del sector energético, entre otros sectores relevantes, así como socios y organismos internacionales.

3. En el presente diagnóstico se implementó como base la Metodología de Madurez de Capacidad de Ciberseguridad (CMM por sus siglas en inglés) edición 2021, desarrollado por el Centro Global de Capacidad de Ciberseguridad (GCSCC, o 'el Centro'), de la Escuela Oxford Martin de la Universidad de Oxford en el Reino Unido. Este modelo define cinco dimensiones de la capacidad de ciberseguridad:

- Política y Estrategia de Ciberseguridad
- Cultura Cibernética y Sociedad
- Desarrollo de Conocimiento y Habilidades en Ciberseguridad
- Marcos Legales y Regulatorios
- Estándares y Tecnologías

4. Cada una de las dimensiones del CMM contiene una serie de factores que describen en detalle, lo que significa tener un nivel avanzado de las capacidades de ciberseguridad. Así mismo, cada uno de esos factores presenta una serie de aspectos que agrupan indicadores relacionados, que describen pasos y acciones que definen

el nivel de madurez de cada aspecto. El modelo del CMM presenta cinco niveles de madurez, que van desde la etapa inicial hasta la etapa dinámica. La etapa inicial implica un enfoque ad-hoc de la capacidad, mientras que la etapa dinámica representa un enfoque estratégico y la capacidad de adaptarse dinámicamente o cambiar en respuesta a los cambios en el entorno del país. Para obtener más detalles sobre las definiciones y la metodología en general, consulte el documento de la metodología del CMM Edición 2021.

5. El Gráfico 1 muestra en términos generales los niveles de madurez de las capacidades de ciberseguridad en Ecuador de las cinco dimensiones, pero con respecto a cada uno de los factores. Cada dimensión representa una quinta parte del gráfico y define los cinco niveles de madurez de cada factor extendiéndose hacia afuera desde el centro del gráfico; el nivel de madurez 'inicial' está más cerca del centro del gráfico y el nivel de madurez 'dinámico' se ubica en el perímetro del gráfico.

Gráfico 1: Representación general de las capacidades de ciberseguridad en Ecuador

Política y Estrategia de Ciberseguridad

6. Ecuador adoptó, mediante el Acuerdo Ministerial 006-2021 de MINTEL, su primera Política Nacional de Ciberseguridad (PNC), la cual fue publicada oficialmente en el Registro Oficial el 13 de junio de 2021. En el proceso de desarrollo de la PNC participaron representantes de instituciones públicas. Sin embargo, la participación del sector privado u otros entes no gubernamentales fue minoritaria. La PNC está orientada principalmente al fortalecimiento de las capacidades de las instituciones del sector público y no se consignaron las prioridades y necesidades de los sectores no gubernamentales.

7. La estructura de gobernanza de ciberseguridad está definida en el Pilar 1 de la PNC, y donde se menciona al Comité Nacional de Ciberseguridad (CNC). Por otro lado, MINTEL tiene varias competencias y funciones relacionadas con la seguridad de la información, pero el mandato del artículo 141 la Ley Orgánica de Telecomunicaciones tampoco es tan amplio para que MINTEL coordine los temas de ciberseguridad a nivel nacional. Varios participantes reconocieron la importancia y necesidad de crear una agencia nacional de ciberseguridad, con poder político y recursos suficientes, que gestione y organice estos temas a nivel nacional.

8. Con respecto al presupuesto para la implementación de la PNC, los ministros responsables de cada pilar deben incluir dentro de su presupuesto anual partidas específicas para atender los objetivos y líneas de acción de la PNC que están bajo su responsabilidad. También se indicó que no existen planes de crear un presupuesto nacional para atender los temas de ciberseguridad. Tanto MINTEL como el CNC planean usar el presente diagnóstico y sus recomendaciones como insumo en el proceso de actualización de la PNC y el desarrollo de la estrategia nacional de ciberseguridad o plan de acción.

9. Ecuador no cuenta con un CERT nacional (Computer Emergency Response Team) que tenga la capacidad y los recursos adecuados para gestionar el ciclo de respuesta a incidentes cibernéticos a nivel nacional. Tampoco cuenta con un registro central donde se identifiquen y categoricen los incidentes cibernéticos a nivel nacional. Ante la necesidad de establecer un CERT nacional en Ecuador, tanto MINTEL como Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) han impulsado al Centro de Respuesta a Incidentes Informáticos del Ecuador (EcuCERT) para que adopte e integre, dentro de su gestión, algunas funciones y responsabilidades que son propias de un CERT nacional; sin embargo, el EcuCERT tiene importantes limitaciones que deben ser solucionadas.

10. El Servicio Nacional de Riesgos y Emergencia (SNRE) es la entidad encargada de garantizar la protección de personas y colectividades de los efectos negativos de desastres de origen natural o antrópico, así como de recuperar y reconstruir las condiciones sociales, económicas y ambientales afectadas por eventuales emergencias o desastres. Sin embargo, la gestión de crisis cibernéticas todavía no se ha integrado a la estructura y políticas de la SNRE.

11. Ecuador no ha identificado formalmente los sectores, subsectores y activos de las infraestructuras críticas a nivel nacional. De conformidad con la PNC, el Ministerio de Defensa Nacional (MDN) es la institución responsable de la protección de las infraestructuras críticas digitales y servicios esenciales en Ecuador (Pilar 3). En el año 2019, se desarrolló una guía para el levantamiento de las infraestructuras críticas, pero es hasta el año siguiente en que el MDN y el Comando de Ciberdefensa (COCIBER), usando una metodología propia, iniciaron el proceso de identificación de las infraestructuras críticas en Ecuador. En dicho levantamiento participaron únicamente las instituciones públicas (telecomunicaciones, sector energético, sector financiero, etc.) y no se tomó en cuenta a las empresas del

sector privado, la cuales también ofrecen servicios críticos y esenciales en el país.

12. El Ministerio de Defensa Nacional (MDN) es el ente rector de la Defensa a nivel nacional, lo cual incluye las operaciones de ciberdefensa. En el año 2021, MDN adoptó la Estrategia de Ciberdefensa, cuyo propósito es el fortalecimiento de la ciberdefensa como una capacidad necesaria para el cumplimiento de la misión constitucional de la defensa y además para desarrollar las capacidades para realizar operaciones de defensa, exploración y respuesta a los efectos producidos por los ciberataques, asegurando una defensa efectiva de las infraestructuras digitales.

13. Por otro lado, el MDN, a través del COCIBER, se realizan evaluaciones de los riesgos cibernéticos, mensualmente o cuando se requieran, para identificar las amenazas a las que está expuesto el país, y dentro del COCIBER, se creó un CERT militar. El CERT militar del COCIBER realiza las actividades de gestión de incidentes, análisis de vulnerabilidades, análisis de malware en dispositivos celulares, y también hacen test de penetración, hackeo ético, entre otros. En cuanto a las operaciones militares, se hacen por defensa y exploración con enlace y respuesta.

Cultura Cibernética y Sociedad

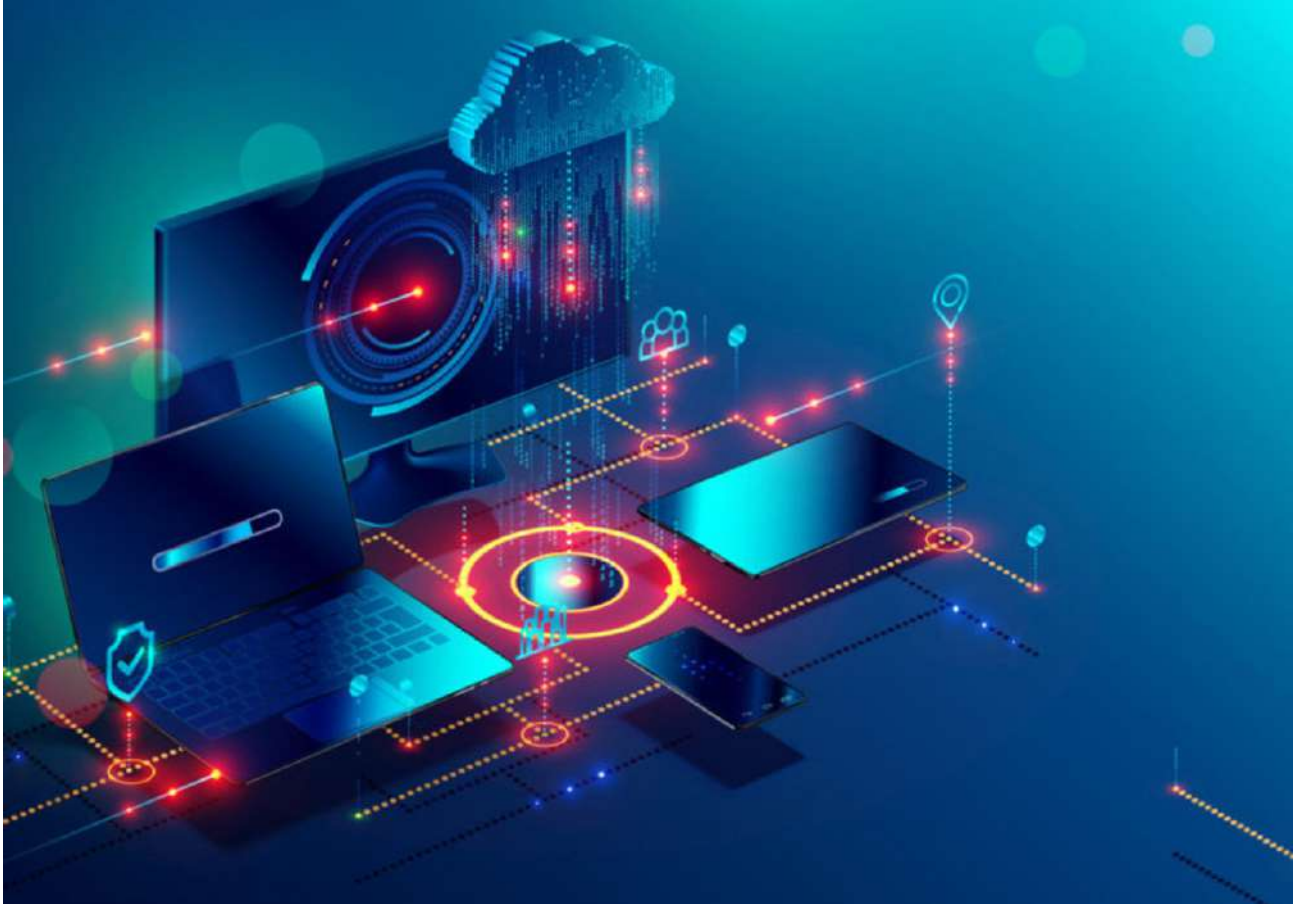
14. Durante el presente diagnóstico se determinó que, el nivel de conciencia y conocimiento sobre los problemas y riesgos de ciberseguridad en Ecuador va en crecimiento, pero todavía no alcanza un nivel adecuado en términos generales.

15. En el sector público, se observa que el nivel de conciencia sobre los riesgos cibernéticos en la mayoría de las instituciones públicas todavía es básico. En el sector privado el nivel de conciencia depende en gran medida del sector o industria y del tamaño de la empresa. Dentro de las empresas grandes o transnacionales, especialmente aquellas empresas que ofrecen servicios financieros, tecnológicos y/o telecomunicaciones, los funcionarios tienen un nivel de conciencia medianamente alto, ya que operan en sectores regulados y regularmente reciben capacitaciones, además de que la misma operación requiere que todos sus empleados tengan un nivel de conciencia adecuado para garantizar la disponibilidad del servicio. En el sector de las Pequeñas y Medianas Empresas (PYMES), el nivel de conciencia puede variar, pero la mayoría de las PYMES realmente no consideran los riesgos cibernéticos como un tema prioritario hasta que ocurre un incidente que las afecte directamente.

16. Con respecto a los usuarios de Internet se determinó que, en términos generales, estos tienen un nivel de conciencia limitado, pero existen factores como el ambiente laboral, grado de escolaridad, etc. que hacen que el nivel de conciencia mejore sustancialmente en ciertos estratos de la población.

17. Estos temas ya han sido identificados por las autoridades competentes e incluso organizaciones del sector privado, académico y sociedad civil. Por tal motivo, se han desarrollado varios programas de alfabetización digital, entre ellos, los implementados en su momento por el Gobierno en los Infocentros y que ahora se llaman Puntos de Encuentro, donde también existen cursos de alfabetización digital más integrales basados en las guías temáticas del PLANADI (Programa Nacional de Alistamiento Digital). MINTEL, en colaboración con otras entidades, desarrolló una aplicación denominada “habilidades digitales”, cuyo objetivo es medir las habilidades digitales de las personas en 5 áreas competenciales específicas, tales como información y alfabetización informacional, comunicaciones y colaboración, creación de contenidos digitales, seguridad de la información y resolución de problemas.

18. En Ecuador no existan evaluaciones o métricas a nivel nacional que determinen el nivel de confianza que



tienen los usuarios de Internet en la información que ven y reciben por medios digitales, como búsquedas en Internet (Google), redes sociales (Facebook, Instagram, Twitter), y otras aplicaciones (WhatsApp), etc.

19. En Ecuador se ha identificado el impacto negativo que generan las noticias falsas y las campañas de desinformación, las cuales amenazan la estabilidad económica, social e incluso la democracia y seguridad nacional, por lo que es recomendable que en la revisión de la PNC se contemple líneas de acciones orientadas a evaluar y establecer políticas públicas y mecanismos legales para contener este tipo amenazas en el país.

20. El Gobierno de Ecuador ha puesto a disposición de la ciudadanía una gran variedad de servicios de gobierno electrónico, los cuales se encuentran disponibles en el siguiente portal web https://www.gob.ec. Dichos servicios van desde páginas meramente informativas hasta plataformas para realizar gestiones y pago de tributos, compras públicas, firma digital, constitución de empresas, ventanilla digital de trámites, entre otras gestiones. Sin embargo, la mayoría de los usuarios ecuatorianos prefieren realizar los trámites de forma presencial debido a que son más fáciles, lo cual indica que todavía no todas las personas entienden el uso de la tecnología y de estas plataformas digitales y/o no confían en ese tipo de plataformas digitales para realizar gestiones de servicios públicos.

21. Las autoridades competentes (e.g., MINTEL, etc.) se toman con seriedad los temas de privacidad, protección de datos personales y seguridad de la información en los portales de gobierno electrónico, por tal motivo, regularmente actualizan sus políticas de privacidad.

22. Los ciudadanos ecuatorianos cuentan con 3 canales para denunciar los delitos informáticos: (1) ante la Fiscalía - Servicios de Atención Ciudadana de la Fiscalía- o a las unidades de Policía Judicial, (2) al número telefónico de emergencias 911, y (3) a la Policía Nacional mediante el número gratuito 1-800 delito donde se reportan todo tipo de delitos, incluyendo los delitos informáticos.

23. Los usuarios de Internet usan las redes sociales e incluso aplicaciones de mensajería instantánea como canales para informar y concientizar a otros usuarios sobre delitos informáticos y otras actividades delictivas. Pocos casos de denunciantes de delitos informáticos que hayan tenido un impacto importante a nivel nacional. Si se observaron más casos de denunciantes de situaciones de noticias falsas o que promueven la desinformación con fines políticos y/o para generar caos.

Desarrollo de Conocimiento y Capacidades en Ciberseguridad

24. Ecuador actualmente no tiene un programa articulado de concientización sobre ciberseguridad a nivel nacional y que esté dirigido a diferentes audiencias, principalmente a grupos o sectores vulnerables: niños, adultos mayores, madres solteras, PYMES, etc. En Ecuador existen varias campañas de concientización que se implementan

de forma independiente (no coordinada) y que son lideradas, principalmente, por MINTEL y otras organizaciones de la sociedad civil, academia, y el sector privado.

25. El nivel de conciencia en temas de ciberseguridad de los ejecutivos y directivos todavía es bajo, ya que desconocen o tienen un conocimiento limitado en temas básicos de ciberseguridad, tales como la necesidad de mejorar la postura de ciberseguridad de las empresas y el impacto de los riesgos cibernéticos en las organizaciones. Ese nivel de conciencia de los ejecutivos mejora en empresas grandes o transnacionales que brindan servicios esenciales.

26. En Ecuador existen profesionales de altísimo nivel en las diferentes disciplinas de la ciberseguridad (técnica, jurídica, etc.); sin embargo, no todos se inclinan por la docencia o no cuenta con las habilidades pedagógicas necesarias, lo cual genera que el cuadro de profesores especializados y calificados en Ecuador sea limitado y actualmente se encuentre topado.

27. Varias universidades a nivel de pregrado y grado, y en carreras específicas, tales como computación, ingenierías, telecomunicaciones, etc. se imparten cursos que abordan temas relacionados con la seguridad de la información, criptografía, seguridad en redes, seguridad y gestión de riesgos en las IT, etc. Sin embargo, en promedio, solo se imparte un curso relacionado con esos temas en toda la carrera, lo cual resulta insuficiente debido a la importancia e impacto que tiene la ciberseguridad en carreras de base tecnológica.

28. En Ecuador existen entre seis o siete programas a nivel de maestría en seguridad informática, ciberseguridad y/o gestión de seguridad de la información -tres programas presenciales y cuatro programas en línea- y que son impartidos por la Universidad Internacional SEK (UISEK), Universidad de las Américas (UDLA), Universidad Internacional de La Rioja (UNIR), Universidad Internacional del Ecuador (UIDE), Universidad Tecnológica Empresarial de Guayaquil (UTEG), Escuela Superior Politécnica del Litoral (ESPOL), y la Pontificia Universidad Católica del Ecuador (PUCE), y algunos casos en colaboración con otras universidades en España. También se indicó que las universidades públicas y privadas no ofrecen becas para los cursos y/o maestrías con énfasis en ciberseguridad. Tampoco existe un programa de becas o fondo de préstamos universitarios enfocados en programas académicos en ciberseguridad.

29. En Ecuador no existen iniciativas o políticas públicas que promuevan o incentiven a los estudiantes y profesionales del sector tecnológico a tomar cursos o iniciar una carrera en el ámbito de la ciberseguridad y/o seguridad de la información. En Ecuador todavía no existe una partida específica dentro del presupuesto nacional para promover e incentivar la educación en ciberseguridad, ni

mucho menos existe una partida dedicada a la investigación y laboratorios en temas de ciberseguridad, aunque según la PNC el tema de la investigación debería ser una prioridad para las universidades u otros centros de formación superior.

30. En Ecuador, el gobierno, la academia y la industria todavía no han conformado un grupo de trabajo para revisar regularmente las prioridades y necesidades del sector. Así mismo, se indicó que esa falta de coordinación a nivel nacional entre dichos sectores se ve reflejada en la PNC, ya que dicha política no cuenta con objetivos estratégicos claros y potentes que aborden las prioridades y necesidades a nivel nacional en el ámbito de la educación de ciberseguridad.

31. En la PNC se documentó que en Ecuador se tiene acceso a certificaciones profesionales en ciberseguridad, pero que la mayoría de esas certificaciones son ofrecidas o administradas por entidades internacionales, lo cual genera dependencia tanto para los profesionales como para las instituciones académicas locales. También existe un desconocimiento sobre la disponibilidad de dichas certificaciones y algunas son demasiado costosas para el público en general, lo cual es una limitante para que más estudiante y profesionales en seguridad se certifiquen.

32. La transferencia de conocimiento en temas relacionados con la ciberseguridad se practica regularmente en Ecuador, principalmente en las empresas del sector privado. En las instituciones públicas no existe una política general en ese sentido; sin embargo, en algunas instituciones se implementa como una buena práctica.

33. En el Pilar 7 de la PNC se estableció que, en las universidades, centro de investigación y otras instituciones académicas, debían incluirse como una prioridad la investigación en temas de ciberseguridad, pero no se crearon objetivos o líneas de acción específicas y robustas en esa línea de trabajo.

Marcos Legales y Regulatorios

34. Ecuador aprobó el Código Orgánico Integral Penal (COIP) en el año 2014, el cual establece la legislación sobre delitos informáticos, incluidas las disposiciones sustantivas (e.g., tipos penales) y las disposiciones procesales (e.g., prueba documental en formato electrónico). De las últimas reformas al COIP se mejoró la legislación de delitos informáticos y se intentó alinear al COIP con la normativa del Convenio de Budapest u otros estándares y buenas prácticas internacionales en materia de delitos informáticos. Pese a lo anterior, Ecuador todavía no es parte del Convenio de Budapest; sin embargo, el Ministerio de Relaciones Exteriores está trabajando en esa línea y recientemente se envió por medios diplomáticos la solicitud formal de adhesión.

35. Dentro de las reformas al COIP (2021) se mejoró la legislación de delitos informáticos relacionada con la

niñez y la adolescencia. Así mismo, el Código de Niñez y Adolescencia no ha corrido con la misma suerte, actualmente se discute en la Asamblea Nacional una reforma integral que dará origen al Código Orgánico de Protección Integral de Niñas, Niños y Adolescentes.

36. Ecuador todavía no se ha realizado una evaluación de impacto para determinar si la actual legislación de delitos informáticos contemplada en el COIP y otras leyes cumple con los estándares internacionales en protección de derechos humanos.

37. Ecuador todavía no cuenta con un marco legal y regulatorio que aborde, de forma integral y de aplicación nacional, requerimientos de ciberseguridad, tales como cumplimiento de estándares de seguridad, notificación de incidentes y/o brechas de seguridad, divulgación de vulnerabilidades, entre otros aspectos.

38. En el año 2021, Ecuador adoptó la Ley Orgánica de Protección de Datos Personales (LOPDP) -publicada en el Registro Oficial Suplemento No. 459 del 26 de mayo del 2021-, la cual entró en vigor desde su publicación y se dio un plazo de dos años de adecuación para entrar a funcionar el sistema sancionatorio. Así mismo, la Constitución Política de Ecuador, en su artículo 66, inciso 19, establece que, a las personas se le reconocerá y garantizará el derecho a la protección de datos de carácter personal.

39. La legislación sobre la defensa al consumidor en Ecuador tiene sustento en la Constitución Política, y la protección del consumidor en línea a nivel general está regulada en la Ley Orgánica de Defensa del Consumidor (2000) y en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002) y su reglamento. La Defensoría del Pueblo, a través de la Defensoría Adjunta del Consumidor y Usuario, es la entidad rectora de la defensa del consumidor en Ecuador. Ecuador cuenta con una Estrategia Nacional de Comercio Electrónico (ENCE).

40. Ecuador aprobó en el año 2021 el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, en donde se regula, en otros temas, el software y bases de datos, tecnologías libres y formatos abiertos, nombres de dominio, entre otros aspectos. Así mismo, Ecuador ha ratificado varios convenios internacionales en el tema en cuestión, pero especialmente los convenios denominados World Intellectual Property Organization (WIPO) Copyright Treaty y el WIPO Performances and Phonograms Treaty, también conocidos como los convenios de Internet por la propia OMPI/WIPO, ya que establecen normas internacionales destinadas a prevenir el acceso no autorizado y el uso de obras creativas en Internet u otras redes digitales. Ecuador ratificó ambos convenios desde el año 2002.

41. En la Policía Nacional existe la Unidad de Delitos Cibernéticos (Unidad especializada). Esta Unidad especializada tiene su centro de operaciones en la ciudad de Quito, pero su jurisdicción sobre delitos cibernéticos es a nivel nacional. Esta Unidad especializada depende financieramente de la Policía Nacional y se cuenta con recursos limitados para la operación. Actualmente, esta Unidad especializada necesita mejorar los recursos y herramientas tecnológicas, tanto hardware como software.

42. La Fiscalía General todavía no tiene una unidad especializada de delitos informáticos y, en términos generales, sus recursos también son limitados. Se analiza la posibilidad de crear una unidad especializada en delitos informáticos para mejorar el servicio. Por otro lado, la mayoría de los jueces desconocen a profundidad los delitos informáticos y los temas técnicos, como el reconocimiento de la evidencia digital. En el país si existen algunos jueces con conocimiento básico y/o avanzado sobre delitos informáticos y evidencia digital, pero quizá por un asunto de competencia y/o jurisdicción -por falta de coordinación administrativa- estos jueces especializados no están conociendo y resolviendo los casos de delitos informáticos.

43. Algunos reguladores sectoriales en Ecuador entienden que deben extender sus actividades de control a temas de ciberseguridad y para ello deben emitir normas técnicas y regulaciones en este campo a efectos de mejo-

rar y garantizar la disponibilidad de los servicios esenciales que ofrecen las entidades reguladas.

44. La Unidad especializada tiene una buena relación con algunos actores del sector privado, especialmente con los operadores de telefonía móvil u otros sectores relevantes, con quienes han desarrollado canales de comunicación y colaboración bastante sólidos.

45. No existe una coordinación interinstitucional ni se ha trazado una hoja de ruta de cooperación entre la Policía Nacional, la Fiscalía General y la Judicatura para mejorar los procesos, comunicación, recursos y conocimiento a efectos ser más eficientes en la investigación y judicialización de los delitos informáticos en el país. Con respecto a la investigación de delitos transfronterizos, esta Unidad especializada tiene una buena relación con sus pares de Colombia y Perú por medio de organismos regionales.

46. La Unidad especializada tiene buena relación con las agencias de cumplimiento de ley internacionales (e.g., INTERPOL, EUROPOL, AMERIPOL, etc.), pero cuando se recurre a mecanismos de asistencia legal mutua para judicializar los requerimientos de información, los plazos son mucho más extenso y poco eficientes -pueden demorar hasta un año la obtención de información.

47. Esta Unidad especializada también trabajan con socios estratégicos, tales como PAcCTO (un programa, financiado por la Unión Europa, de asistencia contra el crimen organizado transnacional), la Embajada de Estados Unidos, la Embajada de Gran Bretaña, entre otros.

Estándares y Tecnologías

48. En Ecuador el cumplimiento e implementación de estándares de seguridad en el ámbito de las tecnologías de la información y la comunicación (TIC) es variado, depende mucho de la naturaleza y tamaño de la organización y el sector en donde opera. Debido a que se están mejorando los niveles de concienciación a nivel corporativo, cada vez más, instituciones públicas y privadas deciden adoptar una postura más responsable, y por ende, comienzan a invertir más recursos en ciberseguridad e implementan este tipo de estándares de seguridad, principalmente como una buena práctica, o incluso porque el mismo mercado demanda ese tipo de actividades para garantizar la disponibilidad del servicio- ya algunos usuarios un poco más sofisticados lo ven como un elemento diferenciador entre los proveedores, pues está en juego su privacidad y la seguridad de sus datos.

49. Las instituciones de la administración pública central están obligadas a cumplir con el Esquema Gubernamental de Seguridad de la Información Versión 2 (EGSI Versión 2.0), y su implementación es supervisada por MINTEL. Actualmente, MINTEL está evaluando a las instituciones públicas que reportaron un nivel de cumplimiento del cien por ciento.

50. Las empresas privadas, catalogadas como grandes y/o transnacionales, principalmente en el sector financiero y telecomunicaciones, tienen un nivel de madurez más avanzado en este ámbito y han desarrollado su propio esquema de seguridad de la información basado en estándares y buenas prácticas internacionales, tales como ISO 27.001, National Institute of Standards and Technology (NIST), entre otras. La implementación de estándares de seguridad en los procesos de compras/adquisición de bienes o servicios es muy similar a lo descrito anteriormente. En términos generales, tanto las instituciones públicas como las organizaciones privadas implementan los lineamientos establecidos por el estándar ISO 27.001 en el ámbito de la relación con proveedores en los procesos de compras de servicios y productos. En Ecuador la implementación de

estándares de seguridad relacionados con la provisión de bienes y servicios es similar o inferior a la implementación de los estándares de seguridad arriba indicados.

51. Ecuador se están implementando una variedad de controles técnicos de seguridad tanto por parte de los usuarios finales como por parte de las instituciones públicas – a través de la implementación de EGSI vo2- y las organizaciones privadas -basadas en el estándar ISO 27.002-, posiblemente no de forma consistente en todos los sectores. Tanto instituciones públicas como organizaciones privadas implementan controles técnicos, tales como antivirus e implementan parches de software -que para muchas instituciones se actualizan automáticamente, procedimientos de administración de contraseñas, así como controles de seguridad física para centros de datos (data centers), y respaldos o copias de seguridad (backups) que se realizan de forma periódica y se almacenan tanto en instalaciones internas como externas.

52. En términos generales, los requerimientos funcionales y de calidad del software en los sectores públicos y privados son reconocidos e identificados, pero no necesariamente de una forma estratégica. El Portal Único de Software Ecuatoriano, es el catálogo único de la oferta de software de cualquier modalidad con valor agregado ecuatoriano mayoritario e importante e integra la información contenida en el catálogo de software publicado en el Sistema de Información de Ciencia, Tecnología, Innovación y Saberes Ancestrales y el catálogo de la oferta nacional de software.

53. Ecuador tiene un mercado de productos y servicios de ciberseguridad pequeño e incipiente, pero activo. Los proveedores de tecnologías de ciberseguridad entienden y reconocen la necesidad de adoptar políticas y procesos seguros durante la etapa de desarrollo, pero no en todos los casos, esos procesos y políticas han alcanzado un nivel operativo. En el caso de productos importados de tecnología de ciberseguridad, la mayoría de los actores del ecosistema entienden que se deben analizar las implicaciones de seguridad, pero no siempre se cuenta con los recursos para tomar las medidas de mitigación que normalmente son ejecutadas dentro de un contexto de cadena de distribución internacional.

54. En Ecuador existen cada vez más consultores independientes y empresas consultoras que ofrecen servicios de consultoría en temas de ciberseguridad tanto para las instituciones públicas como para las organizaciones privadas. Ecuador ya existe un mercado incipiente de ciberseguros a nivel corporativo.

55. En Ecuador todavía no existe un marco legal o regulatorio, de aplicación nacional, que obligue a las instituciones públicas y organizaciones privadas a divulgar las vulnerabilidades, errores y fallas de seguridad y/o a compartir información de incidentes, vulnerabilidades, etc. Debido a lo anterior, tampoco existen mecanismos de protección legal en el ámbito de divulgación responsable de vulnerabilidades.

Reflexión Adicional

56. Es evidente de que el Gobierno del Ecuador está haciendo el mejor esfuerzo para que la ciberseguridad sea una prioridad a nivel nacional y, además, se observó que los otros actores del ecosistema están en esa misma sintonía – solamente necesitan trabajar de forma coordinada en un plan de acción que refleje las necesidades y prioridades a nivel nacional. El Banco Mundial y su equipo de trabajo agradece el apoyo de MINTEL y del Comité Nacional de Ciberseguridad, así como la participación de todos los grupos de interés durante los grupos focales.

METODOLOGÍA

57. Por invitación del Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL) y del Comité Nacional de Ciberseguridad, el Banco Mundial realizó el presente diagnóstico de las capacidades de ciberseguridad de la República del Ecuador. El objetivo de esta revisión es determinar en cuáles áreas el Gobierno de Ecuador podría invertir estratégicamente para mejorar su postura de ciberseguridad nacional.

58. Durante el periodo de diciembre del 2021 a enero del 2022, representantes de los siguientes sectores participaron en varias sesiones virtuales, en las cuales se revisó ampliamente las 5 Dimensiones del modelo CMM:

Gobierno e Instituciones Públicas

- Presidencia de la República
- Ministerio de Relaciones Exteriores
- Consejo de Educación Superior
- Centro de Inteligencia Estratégica
- Ministerio de Defensa
- Ministerio de Gobierno
- Ministerio de Trabajo
- SRI
- DIGERCIC

Ciberdefensa y Seguridad Nacional

- Ministerio de Relaciones Exteriores y Movilidad Humana
- Ministerio de Defensa
- Ministerio de Gobierno
- Centro de Inteligencia Estratégica
- Dirección Nacional de Registros Públicos

Fuerzas de la Ley y Sistema Judicial

- Policía Nacional
- Corte Nacional de Justicia
- Ministerio de Gobierno
- MINTEL

Infraestructuras Críticas #1 Telecom

- CELEC-EP
- CNT
- ETAPA EP
- OTECEL
- ARCOTEL
- CLARO
- ECUCERT

Infraestructuras Críticas #2 Financiero

- BANCO DEL PACÍFICO
- BANCO DE DESARROLLO
- DINERS CLUB
- BIESS
- DINARP
- SUPERINTENDENCIA DE BANCOS
- ASOBANCA
- BANCO DE DESARROLLO
- FEDERACIÓN ECUATORIANA DE TENIS

Infraestructuras Críticas #3 Sector Energético

- Ministerio de Energía y Recursos Naturales No Renovables.
- Empresa Eléctrica Quito EEQ.
- Empresa Eléctrica Centro Sur.
- CNEL EP.
- ARCOTEL
- CELEC EP.

Infraestructuras Críticas #4 Varios Sectores

- Ministerio de Salud Pública.
- Instituto Ecuatoriano de Seguridad Social – IESS.
- Astinave EP.
- Quiport.
- Autoridad Portuaria de Guayaquil.
- Aeropuerto Quito.
- Academia y Sociedad Civil
- Ministerio de Trabajo.

Academia

- Universidad Central del Ecuador.
- Universidad Indoamérica.
- Universidad Técnica del Norte.
- AECI
- Universidad del Azuay
- Senescyt
- Universidad Politécnica Salesiana
- Universidad Internacional del Ecuador
- Escuela Politécnica Nacional
- CACES
- Ministerio de Educación
- Universidad Andina Simón Bolívar
- CSIRT CEDIA

Sector Privado

- CNT
- AECI
- Telconet
- Cámara de Industrias de GYE
- GMS
- DINARP

Grupo Jurídico

- Asamblea Nacional
- Policía Nacional
- Fiscalía General del Estado
- Corte Nacional de Justicia
- CNT-EP
- DINARP
- Corte Nacional de Justicia

Socios Internacionales

- OEA
- BID
- Cyber4dev
- USAID
- Banco Mundial
- ITU

Comité Nacional de Ciberseguridad

- Ministerio de Relaciones Exteriores y Movilidad Humana
- Ministerio de Gobierno
- Ministerio del Interior
- Ministerio de Defensa Nacional
- Ministerio de Telecomunicaciones y Sociedad de la Información
- Centro de Inteligencia Estratégica
- Secretaría General de la Administración Pública de la Presidencia

DIMENSIONES DE LAS CAPACIDADES DE CIBERSEGURIDAD

59. Durante las sesiones de trabajo se implementó la metodología de Madurez de la Capacidad de Ciberseguridad (CMM) del GCSCC, la cual está compuesta por cinco dimensiones que evalúan de forma holística las capacidades de ciberseguridad.

60. Cada dimensión consta de un conjunto de factores, que describen y definen lo que significa poseer una capacidad de ciberseguridad adecuada basada en los cinco niveles de madurez. La siguiente tabla muestra las cinco dimensiones junto con los factores que presenta cada una:

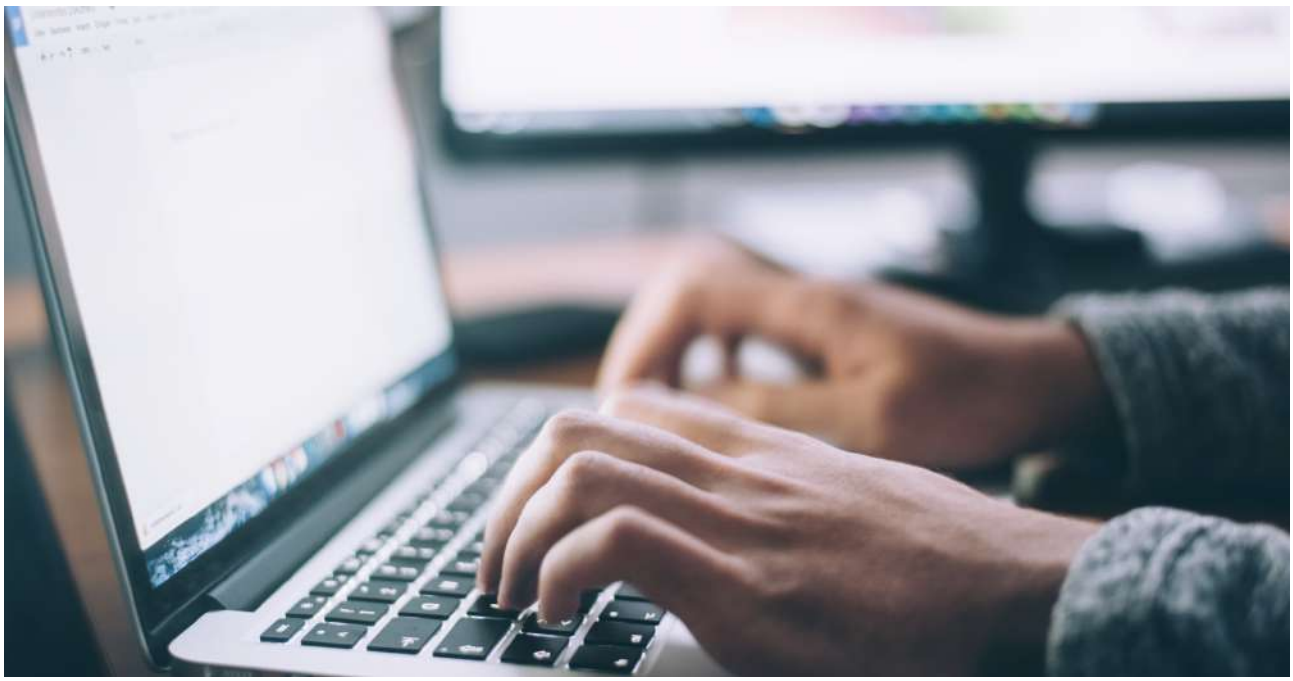
DIMENSIONES	FACTORES
Dimensión 1 Política y Estrategia de Ciberseguridad	D1.1 Estrategia Nacional de Ciberseguridad
	D1.2 Respuesta a Incidentes y Gestión de Crisis
	D1.3 Protección de Infraestructuras Críticas
	D1.4 Ciberseguridad en la Defensa y Seguridad Nacional
Dimensión 2 Cultura Cibernética y Sociedad	D2.1 Mentalidad de Ciberseguridad
	D2.2 Confianza y Creencia en los Servicios en Línea
	D2.3 Comprensión del Usuario sobre la Protección de los Datos Personales en Línea
	D2.4 Mecanismos de Denuncia
	D2.5 Medios de Comunicación y Plataformas en Línea
Dimensión 3 Desarrollo de Conocimiento y Capacidades en Ciberseguridad	D3.1 Desarrollo de Concientización en Ciberseguridad
	D3.2 Educación en Ciberseguridad
	D3.3 Capacitación Profesional en Ciberseguridad
	D3.4 Investigación e Innovación en Ciberseguridad
Dimensión 4 Marcos Legales y Regulatorios	D4.1 Disposiciones Legales y Regulatorias
	D4.2 Marcos Legislativos Relacionados
	D4.3 Capacidad y Competencia Legal y Regulatoria
	D4.4 Marcos de Cooperación Formal e Informal para combatir el Cibercrimen
Dimensión 5 Estándares y Tecnología	D5.1 Cumplimiento de Estándares
	D5.2 Controles de Seguridad
	D5.3 Calidad de Software
	D5.4 Resiliencia de la Infraestructura de Internet y de las Comunicaciones
	D5.5 Mercado de Ciberseguridad
	D5.6 Divulgación Responsable de Vulnerabilidades

DIMENSIONES DE LAS CAPACIDADES DE CIBERSEGURIDAD

61. Cada dimensión contiene una serie de factores que describen lo que significa poseer una capacidad de ciberseguridad adecuada. Cada factor tiene una serie de aspectos que agrupan indicadores relacionados, que describen pasos y acciones que, una vez observados y cumplidos, definen el nivel de madurez de ese aspecto.

62. En el modelo CMM existen 5 niveles de madurez, que van desde el nivel inicial hasta el nivel dinámico. El nivel inicial implica que el país tiene un enfoque ad-hoc de las capacidades, mientras que en el nivel dinámico existe un enfoque estratégico y la capacidad de adaptarse o cambiar dinámicamente frente a las diferentes circunstancias del entorno. Los cinco niveles de madurez se definen de la siguiente manera:

- **Inicial:** en este nivel no existe evidencia de madurez en ciberseguridad, o se encuentra en un estado o nivel embrionario. Puede haber discusiones iniciales sobre el desarrollo de capacidades en ciberseguridad, pero no se han tomado medidas concretas. No existe evidencia de algún tipo de capacidad de ciberseguridad en esta etapa.
- **Formativo:** algunos aspectos han comenzado a crecer y formularse, pero pueden ser ad-hoc, desorganizados, mal definidos o simplemente nuevos; sin embargo, la evidencia de los ligeros avances puede demostrarse claramente.
- **Establecido:** los indicadores del aspecto están establecidos y en modo operativo. Sin embargo, no existe una estructura adecuada con respecto a la asignación de recursos. Se han tomado pocas decisiones con respecto a la inversión y revisión, pero al final el aspecto es funcional y está definido.
- **Estratégico:** en este nivel de madurez, se han tomado decisiones sobre cuáles indicadores del aspecto son importantes y cuáles son menos importantes para la organización o el Estado en particular. Este nivel refleja el hecho de que se han hecho estas elecciones, condicionadas a las circunstancias particulares del Estado u organización.
- **Dinámico:** en este nivel de madurez, existen mecanismos claros para modificar la estrategia según las circunstancias predominantes, como el nivel de sofisticación tecnológica del entorno de las amenazas, el conflicto global o un cambio significativo en un sector sensible (por ejemplo, ciberdelincuencia o privacidad). Las organizaciones dinámicas han desarrollado métodos para cambiar las estrategias de forma pensaba. La toma rápida de decisiones, la reasignación de recursos y la atención constante al entorno cambiante son características de esta etapa.



63. La definición de los niveles de madurez se basa en la evidencia recopilada, incluida la visión general o consensuada de la información presentada por las partes interesadas, la investigación de escritorio realizada y el juicio profesional del equipo de evaluación. En este diagnóstico se presentan los resultados de la evaluación de las capacidades de ciberseguridad de la República del Ecuador y se concluye con una serie de recomendaciones sobre los próximos pasos que podrían considerarse para mejorar las capacidades de ciberseguridad en el país.

METODOLOGÍA PARA MEDIR EL NIVEL DE MADUREZ

64. Durante la presente evaluación, se realizaron múltiples grupos focales, tanto presenciales como virtuales, con actores de los diferentes sectores relevantes del ecosistema. En cada uno de los grupos focales se evaluó una o dos dimensiones de conformidad con el modelo CMM. Así mismo, este diagnóstico tuvo varias novedades en la etapa de implementación. Por ejemplo, se realizaron más grupos focales de los que establece la metodología del CMM. Se realizaron dos grupos focales con los CERTs públicos y privados, dos grupos focales con el sector académico, un grupo focal con solo juristas, cuatro grupos focales con sectores esenciales -para tener un panorama más amplio-, y un grupo focal con los organismos internacionales que está brindando asistencia técnica a Ecuador a efectos de definir las actividades actuales y futuras -para evitar la duplicación de esfuerzos y recursos.

65. Para determinar el nivel de madurez, cada aspecto tiene un conjunto de indicadores correspondientes a los cinco niveles de madurez. Con base en la evidencia recopilada, especialmente durante los grupos focales, se determina cuáles indicadores han sido implementados y eso, a su vez, determinará el nivel de madurez de cada aspecto del modelo. Se utiliza un método de consenso para impulsar las discusiones dentro de los grupos focales.

66. Durante los grupos focales, el equipo de investigadores utiliza preguntas semiestructuradas para guiar las discusiones sobre los indicadores de cada aspecto. Durante estas discusiones, los participantes deben proporcionar la evidencia con respecto a la implementación de esos indicadores, de modo que se minimicen las respuestas subjetivas. Si no se puede proporcionar la evidencia para todos los indicadores en un nivel de madurez, entonces el país en estudio aún no ha alcanzado ese nivel de madurez.

67. El modelo CMM utiliza una metodología de grupos focales, ya que ofrecen la ventaja de recopilar un conjunto de datos con mayor contenido en comparación con otros enfoques cualitativos. Al igual que las entrevistas, los grupos focales son una metodología interactiva con la ventaja de que durante el proceso de recolección de datos e información pueden surgir diversos puntos de vista y concepciones. Lo anterior es parte fundamental de la metodología, ya que en lugar de plantear preguntas a cada entrevistado, el equipo de investigadores deben facilitar la discusión entre los participantes, animándolos a adoptar, defender o criticar las diferentes perspectivas. Usando este tipo de interacción con los participantes se han observado ventajas sobre otras metodologías, posibilitando alcanzar un nivel de consenso entre los participantes y obtener una mejor comprensión de las prácticas y capacidades de ciberseguridad en el país. [4]

68. Con el previo consentimiento de los participantes, todas las sesiones son grabadas y transcritas, y además se implementa la práctica del Chatham House Rule para propiciar un diálogo abierto y franco entre los participantes. El análisis de contenido, una metodología de investigación sistemática utilizada para analizar datos cualitativos se aplica a los datos generados por los grupos focales. El propósito del análisis de contenido es diseñar "inferencias replicables y válidas de los textos al contexto de su uso".[6]

69. Existen tres enfoques para el análisis de contenido. El primero es el enfoque inductivo que se basa en la "codificación abierta", lo cual significa que las categorías o temas son creados libremente por el investigador. En la codificación abierta, los encabezados y las notas se escriben en las transcripciones mientras se leen y se crean diferentes categorías para incluir notas similares que capturen el mismo aspecto del fenómeno en estudio. Se repite el proceso y se vuelven a leer las notas y los encabezados. El siguiente paso es clasificar las categorías en grupos. El objetivo es fusionar posibles categorías que comparten el mismo significado. Dey explica que este proceso clasifica los datos como "que pertenecen juntos".

70. El segundo enfoque es el análisis de contenido deductivo, que requiere la existencia previa de una teoría que sustente el proceso de clasificación. Este enfoque es más estructurado que el método inductivo y la codificación inicial está determinada por las características y variables claves del marco teórico.[4]

71. En el proceso de codificación, los extractos se asignan a categorías y los hallazgos son dictados por la teoría o por investigaciones previas. Sin embargo, podría haber categorías novedosas que pueden contradecir o enriquecer una teoría específica. Por lo tanto, si se siguen estrictamente los enfoques deductivos, estas categorías novedosas que ofrecen una perspectiva refinada pueden ser descuidadas. Esta es la razón por la que el equipo de investigación opta por un tercer enfoque combinado en el análisis de los datos recopilados, que es una mezcla de enfoques deductivos e inductivos.

72. Después de realizar una revisión de la información del país, los datos recopilados durante los grupos focales con las partes interesadas y las notas tomadas durante las sesiones se utilizan para definir los niveles de madurez para cada factor del modelo CMM. El equipo de investigación adopta un enfoque mixto para analizar los datos de los grupos focales y utiliza los indicadores del CMM como criterio para un análisis deductivo. Los extractos que no encajan en los temas se analizan más a fondo para identificar problemas adicionales que los participantes pudieron haber planteado o para adaptar las recomendaciones según el modelo CMM.

73. A la hora de redactar el informe final del diagnóstico, también es necesaria una investigación tanto documental como de escritorio para validar y verificar, e incluso descartar, los resultados. Por ejemplo, es posible que los participantes no siempre estén al tanto de las actualizaciones en el país, por ejemplo, como la promulgación de una ley o reglamento o la adhesión a una convención sobre un tema en particular -protección de datos personales. Las fuentes que pueden proporcionar más información pueden ser los sitios web oficiales del gobierno o ministerios, informes anuales de organizaciones internacionales, sitios web de universidades, etc.

74. Para cada dimensión, se proporcionan recomendaciones accionables sobre los pasos a seguir para lograr una mejora en su capacidad y, por ende, avanzar al próximo nivel de madurez. Si la capacidad de un país para un determinado aspecto se encuentra en un nivel de madurez formativo, al observar el modelo CMM se puede identificar fácilmente los indicadores que ayudarán al país a pasar al siguiente nivel. Así mismo, las recomendaciones también pueden surgir tanto de las discusiones con y entre los participantes como del conocimiento y experiencia del equipo de investigación.

75. Basado en la metodología del CMM, el presente informe presenta los resultados obtenidos durante la evaluación de las capacidades de ciberseguridad de Ecuador, y como se indicó arriba, concluye con una serie de recomendaciones accionables sobre los pasos a seguir para mejorar la capacidad de ciberseguridad en el país.

CONTEXTO DE CIBERSEGURIDAD EN ECUADOR

76. A nivel global, y Ecuador no es la excepción, las TICs han sido fundamentales para la continuidad de las diferentes actividades (e.g., académicas, laborales, salud, entretenimiento, etc.) y el comercio de bienes y servicios durante la pandemia.

77. En el año 2020, la Asociación de Empresas de Telecomunicaciones de Ecuador (ASETEL) y la Asociación de Empresas Proveedoras de Internet, Valor Agregado, Portadores y Tecnologías de Información (Aeprovi) reportaron un crecimiento promedio del 30 % en la demanda del servicio de Internet producto de la crisis sanitaria. Así mismo, MINTEL reportó un incremento del 40 % en el tráfico de la red, lo cual requirió que los operadores de telecomunicaciones tuvieran que cambiar el enrutamiento de sus redes hacia conexiones domiciliarias y además contratar mayor tráfico en el mercado internacional, así como realizar nuevas inversiones en capacidad y redundancia de Internet.

78. A finales del 2021, ARCOTEL reportó que Ecuador presentaba poco más de 12.5 millones de suscripciones de Internet, es decir, una penetración de Internet del 71.7 % por cada 100 habitantes. Durante ese mismo periodo, el acceso a Internet móvil alcanzaba poco más de 10 millones de suscripciones, con una penetración del 57.58 %. Por otro lado, el acceso a Internet fijo en Ecuador llegaba a 2.48 millones de suscripciones en diciembre del 2021, con una penetración del 14.17 %. El Internet de banda ancha fija llega a 2.36 millones de suscripciones, con una penetración del 13.50 %. Así mismo, a inicios del 2022, Ecuador tenía una cobertura móvil de 4G del 85 %.

79. La pandemia también cambió los hábitos de consumo de los ecuatorianos. Según la Cámara Ecuatoriana de Comercio Electrónico (CECE), el consumo a través de medios digitales generó un promedio de USD $2.300 millones; USD $ 700 millones más que en el año 2019. En general, el comercio electrónico creció un 44 %. Según CECE ese crecimiento que se presentó entre el año 2020 y 2021 fue el crecimiento proyectado en los próximos 5 años previo a la pandemia.

80. Así mismo, MINTEL destacó el uso de las TICs, particularmente el uso de trámites en línea y de otros recursos digitales, entre ellas la plataforma gob.ec, como herramientas determinantes para proteger a los ecuatorianos de posibles contagios por aglomeraciones. Así mismo, el uso de las TIC también permitió que los ciudadanos ecuatorianos accedieran a servicios que son indispensables para asegurar su salud, su desarrollo personal y académico, sus actividades productivas, entre otras actividades.

81. Ante ese acelerado crecimiento de las suscripciones de Internet y el alto volumen de transacciones electrónicas y otras actividades en línea, también se incrementaron los amenazas y vulnerabilidades cibernéticas durante la pandemia, poniendo en riesgo tanto al Gobierno, empresas como a los ciudadanos, particularmente cuando se carece una postura de ciberseguridad adecuada. Según la empresa de seguridad Kaspersky, en su reporte Panorama de Amenazas en América Latina 2021, en la región se presentó un crecimiento vertiginoso de los ataques cibernéticos durante la pandemia y Ecuador reportó un alza del 75 % en las incidencias, siendo el país que tuvo el alza más importante en toda la región. Así mismo, la empresa de seguridad ESET reportó en el año 2020 que, Ecuador ocupó la sexta posición dentro de los países latinoamericanos con más detecciones de malware, después de Brasil, México, Argentina, Colombia y Perú.

82. Por otro lado, en el Índice Global de Ciberseguridad del 2020 de la Unión Internacional de Telecomunicaciones, Ecuador figura en el puesto 119 de 130 países que participaron en ese estudio. Ecuador obtuvo un puntaje general de 26.3 de 100 como puntaje máximo. En esa evaluación se revisaron 5 componentes específicos: medidas legales donde obtuvo una puntuación de 10.22, medidas técnicas con un puntaje de 9.55, medidas organizacionales donde obtuvo un puntaje de 0, lo mismo que en medidas de cooperación, y finalmente el componente de desarrollo de capacidad donde se logró un puntaje de 6.53. Con ese puntaje general de 26.3, Ecuador se ubica en el puesto 19 en el ranking de las Américas.

83. En el reporte regional de ciberseguridad 2020 de la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) se desprende que, Ecuador logró un avance discreto en los últimos años, específicamente del 2016 al 2020, en las 5 dimensiones del modelo de CMM, siendo la Dimensión 4 la que presentó un mayor avance durante ese periodo. Por otro lado, la Dimensión 3 no presentó avance alguno durante ese periodo. Mientras que la Dimensión 2 y la Dimensión 5 son las que presentan un nivel de madurez más bajo. La Dimensión 1 tampoco logra un nivel de madurez adecuado.

84. En ese contexto, el Gobierno de Ecuador, en colaboración con los diferentes sectores relevantes del ecosistema, necesita definir una hoja de ruta con objetivos estratégicos claros y recursos suficientes para mejorar sus capacidades de ciberseguridad en el corto y mediano plazo. Justamente ese replanteamiento de objetivos es lo que actualmente MINTEL y otras entidades están realizando con la revisión y actualización de la actual Política Nacional de Ciberseguridad y el desarrollo de la Estrategia Nacional de Ciberseguridad (o plan de acción).

85. En esa línea, el equipo de revisión del CMM notó un ambiente muy positivo durante las sesiones presenciales y virtuales del CMM y un alto nivel de compromiso de todos los sectores, principalmente del Gobierno. Así mismo, el equipo de revisión de CMM y el Banco Mundial esperan que la presente evaluación y sus recomendaciones ayuden a las autoridades competentes de Ecuador a identificar las actuales brechas, prioridades y necesidades nacionales en el ámbito de la ciberseguridad, y también les ayude a tomar decisiones informadas para fortalecer las capacidades de ciberseguridad desde un enfoque holístico y participativo con el fin de promover la prosperidad económica y social de Ecuador.

REPORTE DE REVISIÓN

DESCRIPCIÓN GENERAL

86. Esta sección proporciona una representación general de la capacidad de ciberseguridad en Ecuador. El Gráfico 2 muestra en términos generales los niveles de madurez de las capacidades de ciberseguridad en Ecuador de las cinco dimensiones, pero a nivel de cada uno de los factores. Cada dimensión representa una quinta parte del gráfico y define los cinco niveles de madurez de cada factor extendiéndose hacia afuera desde el centro del gráfico; el nivel de madurez 'inicial' está más cerca del centro del gráfico y el nivel de madurez 'dinámico' se ubica en el perímetro del gráfico.

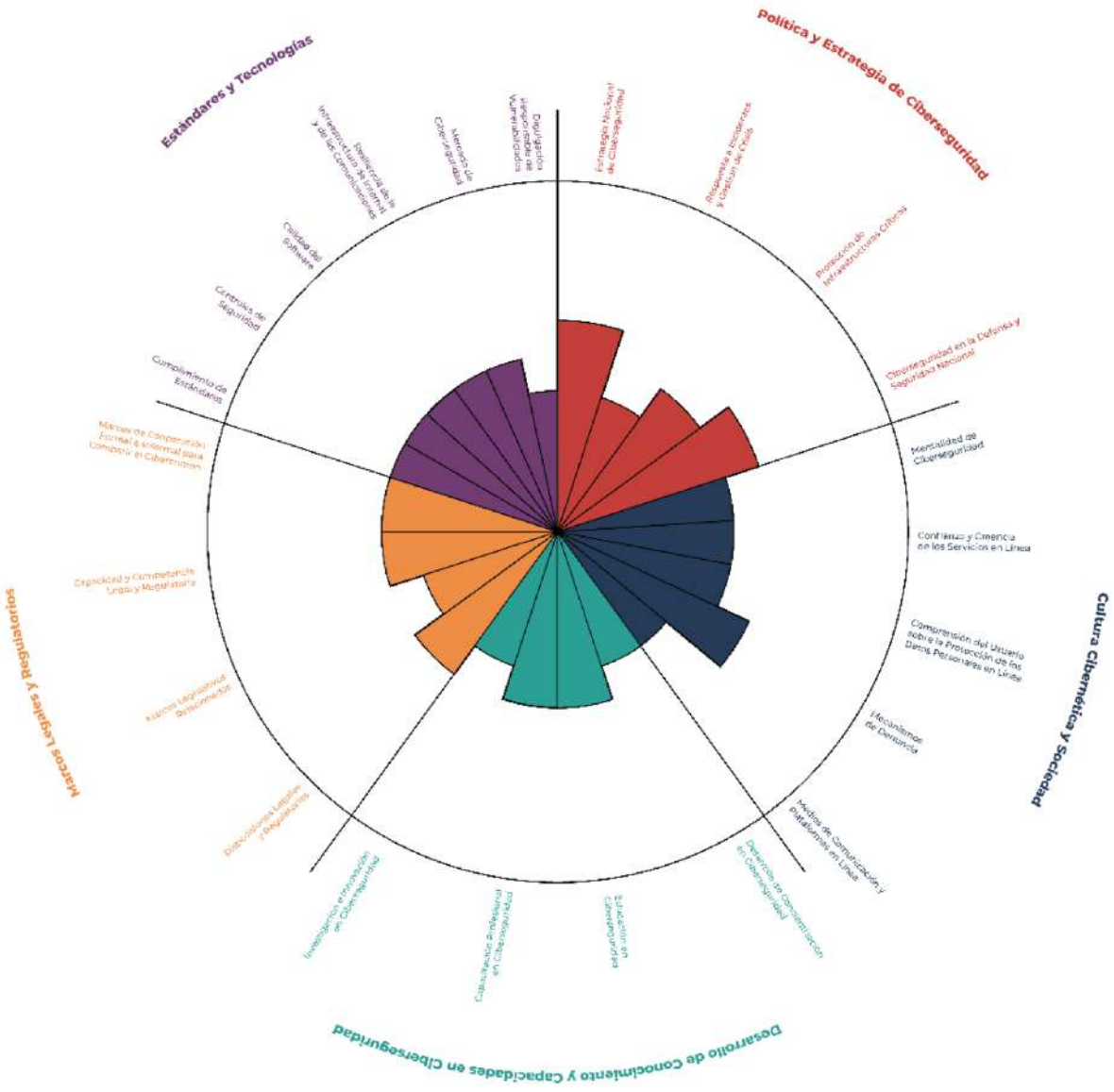
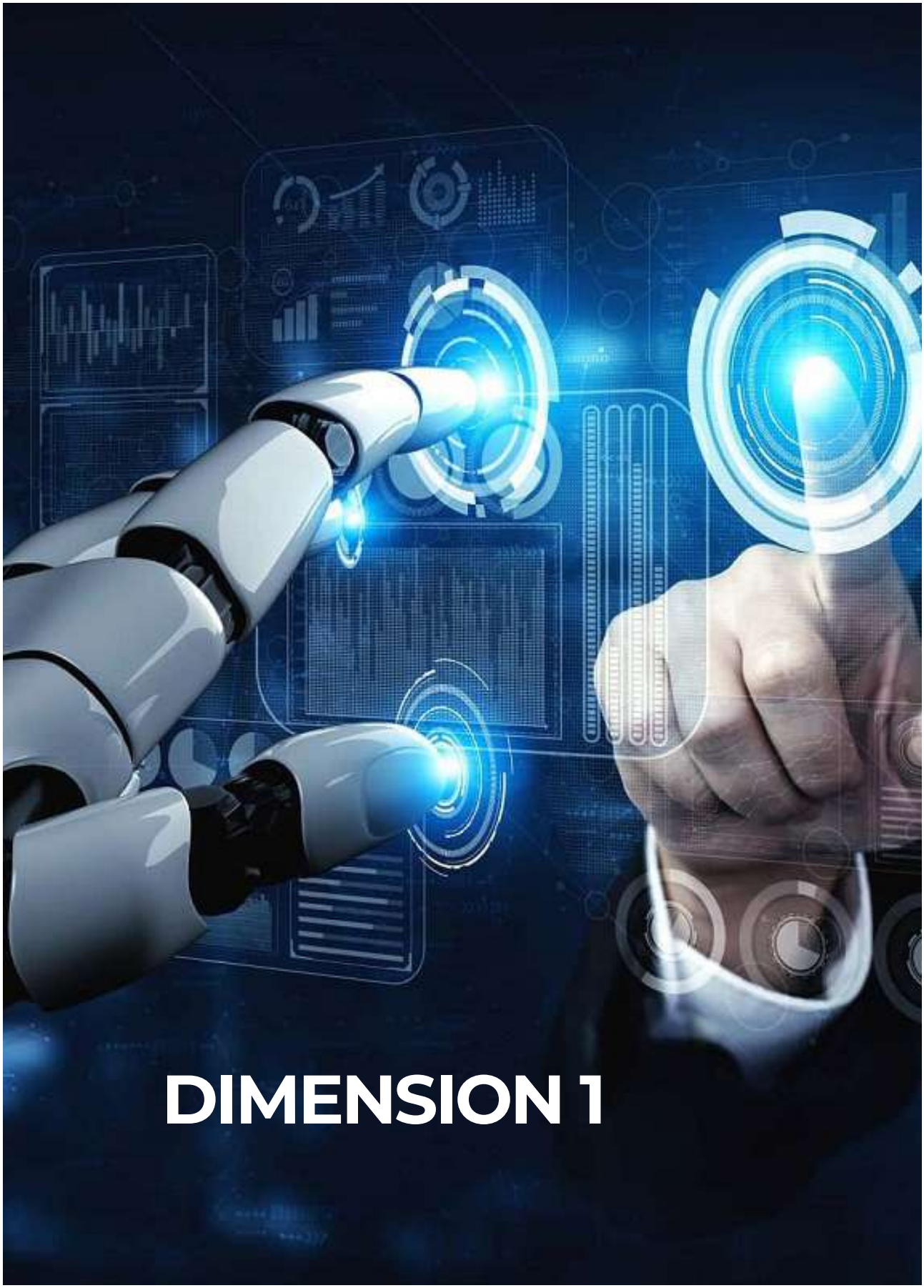


Gráfico 2: Representación general de las capacidades de ciberseguridad en Ecuador



DIMENSION 1

POLITICA Y ESTRATEGIA DE CIBERSEGURIDAD

87. Esta Dimensión evalúa la capacidad que tiene Ecuador para desarrollar e implementar una estrategia nacional de ciberseguridad y mejorar su nivel de ciber resiliencia a través de la mejora de sus capacidades en el ámbito de respuesta a incidentes, gestión de crisis, defensa cibernética y protección de las infraestructuras críticas. Esta Dimensión también evalúa la efectividad de las estrategias y políticas que tienen como objetivo desarrollar capacidades de ciberseguridad a nivel nacional, mientras que se mantienen los beneficios de un ciberespacio que es vital para el funcionamiento del gobierno, las empresas domésticas y transnacionales y la sociedad en general.

La estrategia nacional de ciberseguridad es esencial para definir la hoja de ruta y plan de acción que aborde temas prioritarios de ciberseguridad a nivel nacional, que establezca una estructura de gobernanza con funciones y responsabilidades claras y los mandatos legales de todos los actores clave del ecosistema, lo cual incluye instituciones gubernamentales y no gubernamentales, y además que asigne suficientes recursos para atender los problemas de ciberseguridad tanto emergentes como los existentes, y las prioridades y necesidades de todos los sectores para generar prosperidad económica y social en Ecuador.

D 1.1 ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Nivel de Madurez: Formativo a Establecido (al mes de marzo del 2022)

Establecido (según la actualización que se indica abajo – al mes de agosto del 2022) **

88. La República de Ecuador adoptó, mediante el Acuerdo Ministerial 006-2021 de MINTEL, su primera Política Nacional de Ciberseguridad (PNC), la cual fue publicada oficialmente en el Registro Oficial el 13 de junio de 2021.

89. El MINTEL lideró el proceso de desarrollo de la PNC, a través de un Grupo Interministerial de Ciberseguridad, el cual estuvo conformado por el MINTEL, Presidencia y Vicepresidencia, el Ministerio de Gobierno, el Ministerio de Defensa Nacional, el Ministerio de Relaciones Exteriores y Movilidad Humana, y el Centro de Inteligencia Estratégica (CIES), grupo que fue presidido por MINTEL.

90. Durante el proceso de desarrollo de la PNC -el cual inició en el 2019 y culminó con su aprobación en el 2021-, se realizaron varias actividades, talleres y mesas de trabajo con la asistencia técnica de la Organización de los Estados Americanos, el Banco Interamericano de Desarrollo, una misión técnica del Departamento de Estado de los Estados Unidos (MITRE), u otros socios internacionales.

91. En ese proceso participaron representantes de instituciones públicas. En cuanto a la participación del sector privado u otros entes no gubernamentales fue minoritario, ya que los ministerios coordinadores que existían en aquel momento no tenían rectoría en estos sectores. Algunos participantes reconocen que, si participaron, otros indican que fueron invitados, pero no participaron, mientras que otro grupo de participantes indica que del todo no participaron representantes de sectores no gubernamentales. La mayoría de los participantes coincidieron en que al sector privado no se les dio la oportunidad de realizar comentarios o sugerencias mediante un proceso de consulta pública.

92. Varios participantes también comentaron que la ausencia de los sectores no gubernamentales se ve reflejado en el contenido de la PNC, ya que esta política está orientada principalmente al fortalecimiento de las capacidades de las instituciones del sector público. Así mismo, los sectores no gubernamentales no tienen un papel importante en el proceso de implementación de la PNC. Finalmente, en la PNC no se consignaron las prioridades y necesidades de los sectores no gubernamentales.

93. En las sesiones virtuales se informó que durante el proceso de desarrollo de la PNC no se realizó ninguna evaluación nacional de riesgos cibernéticos.

94. La PNC está basada en siete pilares: 1) gobernanza de la ciberseguridad, 2) sistemas de información y gestión de incidentes, 3) protección de la infraestructura crítica digital y servicios esenciales, 4) soberanía y defensa, 5) seguridad pública y ciudadana, 6) diplomacia en el ciberespacio y cooperación internacional, y 7) cultura y educación de la ciberseguridad. Esos pilares tienen como propósito asegurar la existencia y disponibilidad de las funciones críticas del país, a la vez que promueven eficacia, innovación, comunicación confiable y prosperidad económica y además son consistentes con los valores nacionales y protegen las libertades de los ciudadanos.

95. Esos siete pilares abordan temas sensibles y relevantes a nivel nacional e incluso están alineados con políticas y estrategias nacionales de índole social y económico, tales como la Agenda Digital Ecuador 2021-2022; sin embargo, algunas líneas de acción son limitadas en su alcance, ya que no se le dio el enfoque adecuado para satisfacer las prioridades y necesidades a nivel nacional. Por ejemplo, las líneas de acción relacionadas con la educación en ciberseguridad, la definición de la estructura de gobernanza, entre otros temas. Así mismo, en la PNC no se abordaron temas sensibles, tales como la gestión de la desinformación como una amenaza a la estabilidad economía y social -un asunto sensible en los últimos años, principalmente durante los dos últimos procesos electorales y la pandemia-, la promoción de la igualdad, diversidad e inclusión u otros temas sensibles relacionados con el sector salud y seguridad social -especialmente cuando la dependencia a esas instituciones se incrementó exponencialmente durante la pandemia.

96. En la PNC los mecanismos de seguimiento y monitoreo no están bien definidos y su alcance es limitado. En la PNC se indica que las líneas de acción están planteadas para implementarse en un plazo de 3 años. Así mismo, la PNC sugiere una revisión cada 3 años o cuando se produzca un cambio de mandato institucional. Sin embargo, no se establece un proceso claro, se desconoce cuál institución o comité realizará el monitoreo y la revisión tanto de la PNC como de su implementación. Tampoco indica a cuál institución o comité se reportarán los avances logrados y/o los desafíos o problemas que surjan durante en el proceso de implementación.

97. La PNC tampoco define procedimientos y métricas de revisión para el proceso de implementación de la PNC, que permitan medir el progreso y escalar los riesgos, problemas y dependencias a las autoridades competentes -tampoco esas autoridades están claramente definidas.

98. A la fecha, la PNC no cuenta con un plan de acción o programa de implementación -lo que localmente se denomina la estrategia de ciberseguridad-, que establezca y desarrolle, de conformidad con los estándares y buenas prácticas internacionales, los objetivos y líneas de acción establecidos en los siete pilares de la PNC. Se informó que MINTEL y el CNC están trabajando en la elaboración de este documento.

99. En la PNC se definen los ministerios responsables de cada uno de los pilares, entre ellos figura MINTEL (Pilares 1, 2 y 7), el Ministerio de Defensa Nacional (Pilares 3 y 4), el Ministerio de Gobierno (Pilar 5), y el Ministerio de Relaciones Exteriores y Movilidad Humana (Pilar 6). Así mismo, la PNC establece, de forma muy general, los objetivos y líneas de acción, las metas, indicadores y las entidades responsables; sin embargo, no se hace referencia a temas de presupuesto ni plazos de implementación.

100. La estructura de gobernanza de ciberseguridad está definida en el Pilar 1 de la PNC, y donde se menciona al CNC, como un cuerpo colegiado que tiene como propósito articular los lineamientos y acciones que aportan al fortalecimiento de la ciberseguridad en Ecuador. En sesión formal del Comité Interinstitucional de Ciberseguridad ejecutada el 16 de agosto de 2021 se resuelve la conformación del CNC, el cual está conformado por los cuatro ministerios responsables de los siete pilares más el Centro de Inteligencia Estrategia (CIES). El CNC es presidido por MINTEL y se reúnen cada dos meses aproximadamente.

101. Se informó que en la Asamblea Nacional existen varios proyectos de ley (ver D4) sobre ciberseguridad, pero al menos dos de ellos abordan el tema de la estructura de gobernanza de ciberseguridad a nivel nacional. Sin embargo, no está claro si alguno de esos proyectos de ley está alineado con la estructura que pretende implementar MINTEL y el CNC en Ecuador.

102. Durante las sesiones virtuales del presente diagnóstico se realizó la siguiente pregunta a los participantes, ¿cuál es la institución encargada de la coordinación de los temas de ciberseguridad a nivel nacional? Las respuestas sugerían cierto nivel de confusión; unos decían que MINTEL, otros que el CNC, u otros indicaban que ese tema era confuso, que no estaban definido claramente en ninguna política, decreto o normativa. De hecho, en las sesiones virtuales de las infraestructuras críticas, varios proveedores de servicios esenciales, principalmente del sector financiero y energético, no pudieron dar una respuesta ni mucho menos identificar una estructura de gobernanza.

103. Se mencionó que MINTEL tiene varias competencias y funciones relacionadas con la seguridad de la información, lo cual incluye la implementación de EGSI Versión 2.0, la elaboración y la publicación de la PNC, etc. Sin embargo, el mandato del artículo 141 la Ley Orgánica de Telecomunicaciones tampoco es tan amplio para que MINTEL coordine los temas de ciberseguridad a nivel nacional y, además, interactúe con las organizaciones públicas y privadas. La PNC tampoco es clara en ese sentido y no define cuál institución asumirá ese rol de coordinador nacional.

104. La PNC tampoco establece un programa o esquema donde se definen las funciones y responsabilidades de cada uno de los actores relevantes de la estructura de gobernanza de ciberseguridad. La PNC tampoco aborda temas sensibles como la identificación y dotación de los recursos financieros necesarios para la implementación de la PNC y su estrategia o plan de acción, y a cuáles instituciones públicas se debe escalar, entre otros temas, las deficiencias presupuestarias.

105. Ante esa situación, varios participantes de las sesiones virtuales reconocieron la importancia y necesidad de crear una agencia nacional de ciberseguridad, con poder político y recursos suficientes, que gestione y organice estos temas a nivel nacional. Unos participantes proponen la creación de una secretaria para que comande y lidere estos temas de ciberseguridad a nivel nacional y que MINTEL continúe coordinando los temas técnicos, como la implementación del EGSI Versión 2.0 y el EcuCERT.

106. Varios participantes también señalaron la importancia de integrar más a los sectores no gubernamentales, principalmente al sector privado, academia, sociedad civil, etc., en la estructura de gobernanza de ciberseguridad. La mayoría de los participantes coincidieron en que la es-

tructura de gobernanza de ciberseguridad a nivel nacional debe definirse mediante una ley o decreto ejecutivo e incluso actualmente existen varios proyectos de ley que se discuten en la Asamblea Nacional que abordan este tema. Es importante que MINTEL y el CNC promuevan un proyecto de ley que esté alineado con la estructura, enfoque y actividades que tienen planeadas.

107. En relación con el presupuesto de la implementación de la PNC, varios participantes en las sesiones virtuales indicaron que los ministros responsables de cada pilar deben incluir dentro de su presupuesto anual partidas específicas para atender los objetivos y líneas de acción de la PNC que están bajo su responsabilidad. También se indicó que no existen planes de crear un presupuesto nacional para atender los temas de ciberseguridad.

108. Varios participantes señalaron la necesidad de diferenciar entre los recursos necesarios para atender las necesidades organizacionales en temas de ciberseguridad (e.g., adquisición de firewalls, hardware, software, etc.) de cada institución y los recursos necesarios para implementar los objetivos estratégicos de la PNC. Se indicó que ambos rubros no se pueden mezclar ni debería salir del presupuesto institucional. Así mismo, se comentó que los recursos necesarios para la implementación de la PNC deben provenir de fuentes solventes para asegurar la implementación y sostenibilidad de los objetivos estratégicos como un conjunto.

109. La PNC en su Pilar 6 hace referencia a la cooperación internacional y define tres líneas de acciones, que incluyen la adhesión al Convenio de Budapest, la participación y posicionamiento de Ecuador en foros internacionales y la agenda digital en relaciones bilaterales, regionales y multilaterales, entre otros. A través del Ministerio de Relaciones Exteriores y Movilidad Humana, el EcuCERT, y otras instituciones públicas, Ecuador está participando en grupos y foros internacionales organizados o auspiciados por organismos internacionales, tales como Nacionales Unidas, Banco Mundial, Organización de Estados Americanos, FIRST, CSIRT Americas Network, Internet Governance Forum (IGF), PAcCTO, entre otros, lo cual denota que Ecuador está poco a poco logrando una participación activa en estos foros, generando opciones de colaboración bilateral y multilateral, y un impacto positivo a nivel regional e internacional. Sin embargo, todavía no se ha evaluado la postura de Ecuador ante estos foros y de qué forma los debates internacionales sobre temas de políticas de ciberseguridad y problemas relacionados afectan los intereses y posicionamiento internacional del país.

110. Con la entrada del nuevo gobierno, el tema de ciberseguridad ha tomado un mayor protagonismo en la agenda política. Por ese motivo, MINTEL y el CNC está realizando una revisión o actualización de la PNC, con la asistencia técnica de varios organismos internacionales (OEA, Banco Mundial, MITRE, EU Cyber Resilience for Development- European Union funded project (Cyber4Dev), etc.). En esta oportunidad todos los participantes esperan contar la participación de todos los sectores del ecosistema a efectos de desarrollar una PNC -y su estrategia- con un enfoque holístico y que contemplen las necesidades y prioridades de todos los actores a nivel nacional. Además, de que la realidad de Ecuador en el año 2022 es muy diferente a la de hace dos o tres años, especialmente por la pandemia.

111. A inicios de diciembre del 2021, MITRE, OEA y Banco Mundial colaboraron con MINTEL en la organización de varios talleres con actores del sector público. En uno de los talleres, consultores del Banco Mundial hicieron referencia a la necesidad de revisar la estructura nacional de gobernanza de ciberseguridad y además se indicó que varios objetivos estratégicos de la actual PNC (e.g., protección a las infraestructuras críticas, educación en el ámbito de la ciberseguridad, etc.) carecían de contenido, ya que no tenían un enfoque integral y de prioridad nacional. Así mismo, MITRE realizó un diagnóstico en donde se concluyó (in-situ) que los actuales 7 Pilares de la PNC son pertinentes; sin embargo, si es necesario modificar los objetivos estratégicos de cada pilar para que sea más integral su enfoque – Reporte Final de MITRE todavía no ha sido presentado a MINTEL.

112. Así mismo, tanto MINTEL como el CNC planean usar el presente diagnóstico y sus recomendaciones como insumo en el proceso de actualización de la PNC y el desarrollo de la estrategia nacional de ciberseguridad o plan de acción.

****Actualización**

El Gobierno de Ecuador aprobó la nueva Estrategia Nacional de Ciberseguridad 2022-2025, mediante la Resolución No. CNC-2022-007 del 3 de agosto del 2022 del Comité Nacional de Ciberseguridad.

A solicitud de MINTEL y basado en información suministrada por dicho ministerio, se actualiza la Dimensión 1, específicamente el factor D.1.1 "Estrategia Nacional de Ciberseguridad", sustentada en los siguientes avances:

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) en su visión de fortalecer la ciberseguridad del país ha trabajado de manera conjunta con el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA) y el Proyecto CYBER4DEV de la Unión Europea para el desarrollo de la "Estrategia Nacional de Ciberseguridad de Ecuador", con la valiosa participación del CNC, Funciones del Estado, instituciones públicas, sector privado, academia, sociedad civil y otros actores relevantes.

La Estrategia Nacional de Ciberseguridad del Ecuador (ENC) fue aprobada mediante Resolución No. CNC-2022-007 del 3 de agosto del 2022 del CNC, la misma que se encuentra en el portal de Gobierno Electrónico (https://www.gobiernoelectronico.gob.ec/estrategia-nacional-de-ciberseguridad-del-ecuador/). Es importante señalar que las autoridades competentes (e.g., MINTEL, CNC, EcuCERT) deberían diseminar ampliamente la ENC en todos los sectores.

En términos generales, la ENC define el panorama nacional de ciberseguridad, desafíos y oportunidades, la visión, principios rectores y objetivos estratégicos. Asimismo, la ENC establece los siguientes seis pilares y sus objetivos estratégicos:

- **PILAR 1:** Gobernanza y coordinación nacional.
- **PILAR 2:** Resiliencia Cibernética.
- **PILAR 3:** Prevención y combate a la ciberdelincuencia
- **PILAR 4:** Ciberdefensa
- **PILAR 5:** Habilidades y capacidad de ciberseguridad
- **PILAR 6:** Cooperación internacional

Finalmente, la ENC establece un apartado sobre la implementación, seguimiento y evaluación.

Durante el desarrollo de la ENC no se realizó una evaluación nacional de riesgos cibernéticos, por lo que su contenido no está basado en una evaluación de esa naturaleza. Sin embargo, uno de sus pilares, particularmente la Resiliencia Cibernética (Pilar 2), propone adoptar un enfoque basado en gestión de riesgos a todo nivel. Por otro lado, el contenido de la ENC está alineado con otras políticas y estrategia nacionales de índole socioeconómico. Asimismo, la ENC refleja las necesidades y funciones de los principales actores del ecosistema, incluyendo al sector público, sector privado, academia, y sociedad civil.

El contenido de la ENC incluye acciones relacionadas con el establecimiento de una estructura de gobernanza (Pillar 1), la concientización tanto del público en general como del sector empresarial (Pilar 5), mitigación de la cibercriminalidad (Pilar 3), establecimiento y fortalecimiento de la capacidad de respuesta a incidentes cibernéticos (Pilar 2), protección a las infraestructuras críticas (Pilar 2), promoción de la cooperación internacional (Pilar 6) y de las alianzas público-privadas (principio rector "visión inclusiva y colaborativa"), entre otros aspectos. La ENC no incluye, al menos de forma expresa, temas relacionados con la protección de la niñez en línea y la mitigación de la desinformación – este último un tema bastante crítico en Ecuador según lo identificado en el presente diagnóstico. La ENC promueve el respeto y protección de los derechos humanos, particularmente en el principio rector "salvaguardar los derechos digitales". En el principio rector "visión inclusiva y colaborativa" se incluyen aspectos de inclusión y participación de todos los actores relevantes del ecosistema y promoción de la cooperación nacional e internacional y otras alianzas estratégicas.

En el Pilar 1 se establece la necesidad de definir un marco integral de gobernanza y coordinación nacional, así como desarrollar un marco legal y regulatorio integral que sustente el desarrollo e implementación de la estructura de gobernanza nacional de ciberseguridad y de la ciberdefensa -el cual deberá establecer con total claridad las funciones y responsabilidad de los actores relevantes de la estructura de gobernanza y la asignación de recursos para su adecuado funcionamiento. Actualmente, MINTEL es el ministerio rector y el CNC opera como el órgano estratégico de coordinación y toma de decisiones. La implementación de la ENC estará a cargo del CNC con apoyo de las instituciones con competencias en la seguridad integral del Estado. Asimismo, la ENC señala que la responsabilidad de la efectiva implementación de las iniciativas y acciones recae en cada una de las múltiples partes interesadas del ecosistema de ciberseguridad de Ecuador.

La propia ENC reconoce como desafío el tema de asignación de recursos financieros. Sin embargo, indica que los objetivos estratégicos se cubrirán mediante la planificación presupuestaria tanto en términos de gastos de funcionamiento como de inversiones específicas, incorporando el presupuesto nacional y los mecanismos de apoyo. También señala que las fuentes de financiación podrían ser internas o de donantes internacionales. No queda claro, pues no está expresamente indicado en la ENC, el proceso de esca-

lamiento y de toma de decisión al más alto nivel ante una situación de deficiencia presupuestaria. Se recomienda incluir este procedimiento de forma detalla en el plan de acción de la ENC.

La ENC indica que se elaborará un plan de acción con acciones y actividades concretas que se llevaran a cabo para alcanzar los objetivos estratégicos. Este plan de acción estará sujeto a las modificaciones que apruebe el CNC a medida que avance la implementación de la ENC. Se espera que en el desarrollo del plan de acción igualmente participen todos los actores relevantes del ecosistema y que estos tengan un rol activo en el proceso de implementación de los objetivos estratégicos. Se estima que el plan de acción estará finalizado y debidamente publicado en el mes de febrero del 2023.

Como se indicó anteriormente, la ENC tiene un apartado sobre mecanismos y procesos de monitoreo de los resultados alcanzados y abordaje de los problemas de implementación a efectos de conservar la línea rectora de la ENC. Asimismo, en este apartado se definen una serie de indicadores para medir la evolución y rendimiento del proceso de implementación de los objetivos estratégicos. Se prevé una revisión y actualización de la ENC cada tres años o según se considere necesario. Incluso, la ENC indica que se creará y ejecutará un plan estratégico de comunicación del cumplimiento de los objetivos de la ENC, en donde se establecen tareas y acciones específicas que se realizarán en el marco de los procesos de implementación, seguimiento y monitoreo. Se estima que este plan estará finalizado en el mes de febrero del 2023.

En cuanto a la participación e involucramiento de Ecuador en el plano regional e internacional, el país todavía no ha realizado una evaluación de impacto para medir de qué forma los debates internacionales sobre políticas de ciberseguridad y temas afines afectan los intereses del país. Sin embargo, Ecuador, por medio de la Cancillería y otras instituciones, está trabajando en el escenario internacional. Por ejemplo, Ecuador está participando activamente en el proceso de desarrollo de la nueva convención sobre cibercriminalidad de las Naciones Unidas. Asimismo, ya inició el proceso de adhesión a la Convención de Budapest del Consejo de Europa.

En enero del año 2022, MINTEL anunció que Ecuador será una subsede de Cyber4Dev para la región Andina. Este proyecto convertirá a Ecuador en un referente y centro de capacitación y formación en temas de ciberseguridad a nivel regional.

En el mes de septiembre del año en curso, una comitiva de representantes ecuatorianos participó en un tour de estudio en Tallin, Estonia, con los siguientes logros obtenidos:

- Se conoció la experiencia de Estonia en la implementación de temas como gobierno digital, ciberseguridad a través de los proyectos presentados en desarrollo en innovación y transformación digital.
- Se mantuvo reuniones con los diferentes entes gubernamentales y empresas privadas de Estonia vinculados en temas de Ciberseguridad, en donde se conoció las mejores experiencias y buenas prácticas aplicadas en dicho país.
- Se obtuvo una visión holística de la seguridad, enfocada a la ciberseguridad, así como el blindaje tecnológico a los sistemas e infraestructuras críticas del Ecuador.
- Se adquirió nuevos conocimientos técnicos y uso de herramientas presentadas que servirán para fortalecer la seguridad y garantizar una resiliencia cibernética.
- Se obtuvo una perspectiva integral, así como conocimientos prácticos que se podrán incorporar en las labores profesionales.

La Autoridad de Sistemas de Información de la República de Estonia (RIA) ejecutora del proyecto EU CYBER CAPACITY BUILDING NETWORK (EU CyberNet) y en representación del Gobierno del Ecuador, el Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH) y el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), firmaron el 27 de abril de 2022, un Memorando de Entendimiento, que tiene por objeto reflejar las intenciones de las partes de coordinar para la subregión Andina, las actividades de cooperación internacional del EU CyberNet, en el marco del proyecto LAC4. A través del HUB PARA LA SUBREGIÓN ANDINA ESTABLECIDO EN EL ECUADOR. Ya se han realizado capacitaciones y seminarios en el mes de agosto y de septiembre del presente año.

Este Factor evalúa la capacidad del Gobierno de Ecuador para identificar y determinar las características de los incidentes a nivel nacional de manera sistemática. También revisa la capacidad del gobierno para organizar, coordinar y hacer operativa la respuesta a incidentes, y si la ciberseguridad se ha integrado en el marco nacional de gestión de crisis.

D 1.2 RESPUESTA A INCIDENTES Y GESTION DE CRISIS

Nivel de Madurez: Formativo

113. Ecuador no cuenta con un CERT nacional que tenga la capacidad y los recursos adecuados para gestionar el ciclo de respuesta a incidentes cibernéticos a nivel nacional. Tampoco cuenta con un registro central donde se identifiquen y categoricen los incidentes cibernéticos a nivel nacional.

114. En el año 2014, la Superintendencia de Telecomunicaciones constituyó formalmente el EcuCERT como un centro de respuesta a incidentes para el sector de telecomunicaciones; sin embargo, el EcuCERT había iniciado operaciones desde el año 2013. En el año 2015, con la promulgación de la Ley Orgánica de Telecomunicaciones se creó ARCOTEL y este ente asumió la administración del EcuCERT.

115. Ante la necesidad de establecer un CERT nacional en Ecuador, tanto MINTEL como ARCOTEL han impulsado al EcuCERT para que adopte e integre, dentro de su gestión, algunas funciones y responsabilidades que son propias de un CERT nacional; sin embargo, el EcuCERT tiene importantes limitaciones que deben ser solucionadas.

116. Aún sin tener el mandato legal y los recursos adecuados, la PNC explícitamente reconoce que el EcuCERT es la estructura de coordinación nacional para el manejo de incidentes de seguridad de la información -así se establece en la página 34 de la PNC. En las sesiones virtuales se mencionó en reiteradas ocasiones que, la carencia de un mandato legal expreso y el vínculo directo con el sector de telecomunicaciones generaba cierta disconformidad tanto en las instituciones públicas como en las organizaciones privadas, aunado a que su capacidad operativa es muy limitada.

117. El EcuCERT depende financieramente de ARCOTEL y tiene un staff de nueve profesionales con formación en varias ingenierías, tales como electrónica, telecomunicaciones y en sistemas. Varios miembros del staff cuentan con más de una maestría en seguridad de la información y poseen certificaciones de la industria, tales como CH4- la cual por un tema de presupuesto no se pudieron renovar recientemente.

118. El EcuCERT cuenta con recursos tecnológicos limitados; su infraestructura y equipo se adquirió en el año 2013 y desde el año 2018 se ha tratado de actualizarlo sin éxito. Una limitante que tiene el EcuCERT, y posiblemente todas las instituciones públicas, es el tema de la territorialidad de los datos, impidiendo la contratación de servicios en la nube. Actualmente, el EcuCERT opera con un

equipo tecnológico que ya no cuenta con soporte técnico del fabricante, por lo que se están tercerizando algunos servicios (e.g., seguridad perimetral) para garantizar la continuidad de la operación. En las sesiones virtuales se indicó que MINTEL tiene planes de establecer un Security Operations Center (SOC), el cual sería gestionado por el EcuCERT, justamente para darle más herramientas y mejorar su capacidad en el ámbito de respuesta a incidentes.

119. Se informó que El EcuCERT, al igual que otras instituciones públicas, debe contar con un plan de capacitación para sus funcionarios -por disposición del Ministerio de Trabajo-; sin embargo, ese plan no se ha cumplido por falta de presupuesto. Actualmente, los miembros del EcuCERT recurren a capacitaciones, cursos u otros recursos de formación gratuitos para mantenerse actualizados. Se comentó que en el pasado el EcuCERT invirtió recursos en la capacitación de su staff; sin embargo, varios funcionarios, pocos meses después, se marcharon al sector privado, perdiéndose la inversión en capacitaciones.

120. En una de las sesiones virtuales se indicó que el EcuCERT brinda tres servicios generales: reporte de incidentes; capacitación y concientización; y monitoreo y alertas tempranas, siente esta último su principal función. El EcuCERT no funciona como un registro central de incidentes, pero tiene varios proveedores de feeds o

alertas, las cuales son notificadas a los operadores de telecomunicaciones y algunas otras instituciones con las cuales han establecido un convenio de colaboración. El EcuCERT está ofreciendo esos tres servicios a varias entidades bancarias estatales.

121. En cuanto a la capacidad de gestión de respuesta a incidentes, se indicó en las sesiones virtuales que el EcuCERT tiene varios protocolos debidamente establecidos y documentados, los cuales se desarrollaron cuando se obtuvo la certificación de FIRST en el año 2014. Hace un tiempo se hizo una actualización de esos protocolos de conformidad con la norma técnica adoptada por ARCOTEL en relación con la gestión de incidentes y vulnerabilidades. Esos protocolos fueron aprobados por las autoridades competentes, y en el año 2021 se realizó una actualización de algunos procedimientos y documentos, entre ellos el manual de triage.

122. Actualmente, solo los operadores de telecomunicaciones tanto públicos como privados y aquellas instituciones públicas y privadas que han sufrido una brecha de seguridad de conformidad con la Ley Orgánica de Protección de Datos Personales (art. 43), tienen la obligación de reportar esos incidentes a ARCOTEL a través del EcuCERT y a la Superintendencia de Protección de Datos – la cual todavía no ha sido formalmente conformada.

123. A nivel del sector de telecomunicaciones, ARCOTEL emitió una norma técnica (No. 2018-0652) que establece los lineamientos sobre la gestión de incidentes y vulnerabilidades, lo cual incluye un catálogo de incidentes y niveles de priorización. En el caso del sector financiero, la Superintendencia de Bancos también obliga a las entidades financieras a reportar los incidentes en general, incluyendo incidentes cibernéticos, que causen la indisponibilidad del servicio.

124. En Ecuador no existe normativa expresa que obligue a las organizaciones públicas y privadas a reportar los incidentes cibernéticos a las autoridades competentes. Sin embargo, MINTEL, en su condición de ente rector del EGSI Versión 2.0, emitió un oficio, sustentado en el artículo 140 y 14 de la Ley Orgánica de Telecomunicaciones, para que las instituciones de la Administración Pública dependientes de la Función Ejecutiva notificarán los incidentes cibernéticos al EcuCERT, pero existen dudas sobre la obligatoriedad de esa notificación al EcuCERT. Mediante Oficio No. MINTEL-2021-0312-O del 23 de julio de 2021, emitido por la Dra. Vianna di María Maino Isaías, Ministra de Telecomunicaciones y de la Sociedad de la Información, se presentan las recomendaciones preventivas y correctivas de ciberseguridad y se solicita se realice las respectivas acciones técnicas. Así mismo, mediante Oficio No. MINTEL-2021-0313-O del 23 de julio de 2021, emitido por la Dra. Vianna di María Maino Isaías, Ministra de Telecomunicaciones y de la Sociedad de la Información, se presentan las medidas preventivas y correctivas ante posibles ataques de Ransomware y se solicita se realice las respectivas acciones técnicas.

125. Parte de los cambios que deben darse para fortalecer las capacidades del EcuCERT, es dotarlo de las herramientas técnicas y legales para que tanto las instituciones públicas como las organizaciones privadas reporten sus incidentes de forma obligatoria. Varias organizaciones públicas y privadas, principalmente con las que se tiene un convenio o forman parte de la Red Nacional de Confianza (RNC), si realizan dichos reportes de forma voluntaria.

126. El EcuCERT ha establecido varios canales de comunicación para el intercambio de información, principalmente con instituciones públicas y los miembros RNC, así como los protocolos para garantizar la confidencialidad de la información que se comparte por esos canales. En el año 2020, se creó un proyecto que fue avalado por las autoridades de ARCOTEL para constituir la RNC, como una plataforma voluntaria y colaborativa, en la cual participan siete CERTs públicos y privados de Ecuador, los cuales deben cumplir con una serie de requisitos y suscribir un acuerdo de no divulgación de la información.

127. A través de la RNC se ha facilitado la gestión de incidentes críticos y además se puede compartir información sobre incidentes y vulnerabilidades. Los miembros de la RNC reciben constantemente soporte técnico y lineamientos para mejorar su ciclo de gestión de incidentes, permitiendo mejorar sus capacidades internas. Como parte de la RNC, existe un chat en una aplicación de mensajería instantánea que opera bajo los protocolos del Traffic Light Protocol e incluso, cierta información de tipo confidencial o sensible es compartida en formato encriptado. Como parte de las actividades de la RNC, el EcuCERT ha organizado talleres de Sim3 para que esos CERTs se autoevalúen y determinen su nivel de madurez.

128. Ante la necesidad de contar con un CERT nacional con los recursos adecuados, tanto MINTEL, ARCOTEL como el mismo CNC tienen claro que deben trabajar en la línea de la transformación del EcuCERT, y para ello, deben darle las herramientas técnicas y legales para que opere como un CERT nacional.

129. En las sesiones virtuales se indicó que ARCOTEL y EcuCERT están trabajando con la Unión Internacional de Telecomunicaciones (UIT) en una evaluación de las capacidades del EcuCERT a efectos de determinar cuáles mejoras deben realizarse a nivel de recurso humano, financiero y tecnológico para que vaya asumiendo progresivamente y ejecutando las funciones y responsabilidades de un CERT nacional. En el pasado, la agencia Cyber4Dev realizó una evaluación de las capacidades del EcuCERT, pero desde la óptica de un CERT sectorial.

130. En el año 2017, el Banco Interamericano de Desarrollo (BID) realizó una evaluación y en su reporte final se establecieron los lineamientos de cómo debería funcionar un CERT nacional en Ecuador. Producto de esa evaluación, ARCOTEL ya tiene cuantificado los costos de inversión para mejorar las capacidades del EcuCERT y se estima que ese proceso de transformación podría concluir en el año 2025.

131. A pesar de todas las limitaciones del EcuCERT, este centro de respuesta a incidentes ha sabido posicionarse a nivel internacional. Desde el año 2014 forma parte de la comunidad de FIRST y además ha logrado participar activamente en grupos y foros regionales e internacionales, donde se comparte información de incidentes, vulnerabilidades e incluso se comparten buenas prácticas en diferentes temas. Así mismo, el EcuCERT ha desarrollado una relación colaborativa y dinámica con CERTs regionales y CERTs de países vecinos.

132. También se determinó que la mayoría de las principales organizaciones tanto públicas como privadas han desarrollado mecanismos internos para gestionar los incidentes, lo cual incluye los procesos de identificación, categorización, contención y recuperación. Algunas organizaciones, como empresas grandes o transnacionales, tienen sus propios recursos internos o desde la casa matriz u oficina regional se brinda ese soporte técnico, mientras que otras empresas tercerizan los servicios de SOC. En la mayoría de los casos, las organizaciones recurren a la tercerización de esos servicios, ya que no cuentan con personal calificado y las herramientas tecnológicas adecuadas.

133. En el sector financiero, la Superintendencia de Bancos y la Asobanca han explorado la posibilidad de crear un CERT sectorial, pero a la fecha esa iniciativa todavía no ha prosperado. También en el sector energético se han hecho esfuerzos para establecer un CERT sectorial. Por ejemplo, Corporación Eléctrica del Ecuador (CELEC) tiene un CERT con un nivel operativo aceptable y en el pasado se conversó sobre la posibilidad de ampliar la comunidad objetivo para cubrir todas las empresas del sector eléctrico. Debido a cambios gerenciales en la estructura de CELEC, la iniciativa quedó suspendida, pero si existe disposición por parte de CELEC de colaborar con las otras empresas del sector. Se mencionó que las autoridades competentes deberían darles seguimiento a esas dos iniciativas.

134. También se indicó que, el principal problema radica en las PYMES, donde existe un nivel bajo de concientización en temas de ciberseguridad y no todas las empresas cuentan con recursos, profesionales en informática y protocolos de seguridad para identificar y contener los incidentes cibernéticos, así que el nivel de vulnerabilidad de este sector es alto. Sin embargo, en una de las sesiones virtuales se indicó que el costo de los servicios SOC es asequible y están disponibles incluso para las PYMES. Se estima que un 60 % de las empresas catalogadas como PYMES tienen la posibilidad de subcontratar servicios de monitoreo y de respuesta a incidentes, pero se debe trabajar más en el tema de la concientización. Con la entrada en vigor de la Ley Orgánica de Protección de Datos y su reglamento más organizaciones públicas y privadas se ven forzadas a mejorar sus capacidades internas o a subcontratar esos servicios de monitoreo y respuesta a incidentes.

135. Pese a los esfuerzos individuales que tanto las instituciones públicas como privadas realizan para desarrollar capacidades en el ámbito de respuesta a incidentes, la carencia de un ente de coordinación nacional, que en principio debería ser el EcuCERT, limita las capacidades de coordinación y mitigación a nivel nacional.

136. En varias sesiones virtuales, varios participantes de diferentes sectores señalaron que el EcuCERT debe resolver los siguientes desafíos:

- Se debe ampliar la comunidad objetivo -no solo el sector de telecomunicaciones.
- Contratar más personal capacitado y mejorar el plan de capacitación de su personal en general.
- Ampliar el horario de funcionamiento, actualmente tiene horario de oficina 8x5, cuando cualquier CERT nacional debe trabajar 24x7.
- La dependencia con ARCOTEL y MINTEL, limita sus funciones, algunos sugieren que debe salir de ARCOTEL para que tenga mayor independencia.
- Debe mejorar la confianza con las comunidades objetivo.
- Brindar acompañamiento.

137. En Ecuador, el Servicio Nacional de Riesgos y Emergencia (SNRE) es la entidad encargada de garantizar la protección de personas y colectividades de los efectos negativos de desastres de origen natural o antrópico, así como de recuperar y reconstruir las condiciones sociales, económicas y ambientales afectadas por eventuales emergencias o desastres. Sin embargo, la gestión de crisis cibernéticas todavía no se ha integrado a la estructura y políticas de la SNRE.

138. Se comentó que, MINTEL, CNC y otras autoridades competentes entienden la necesidad de establecer un

plan nacional de gestión de crisis. Por tal motivo, en el año 2020, MINTEL coordinó la redacción de un protocolo para gestionar crisis cibernéticas a nivel nacional; sin embargo, esta iniciativa no prosperó debido a la falta de claridad en cuanto a los roles, funciones y responsabilidades de cada institución involucrada en el proceso de gestión de crisis cibernéticas – problema que no se resolverá hasta que se tenga bien definida la estructura de gobernanza de ciberseguridad. En su momento se había acordado de que una vez que el CNC se estableciera formalmente -lo cual ya sucedió-, ese protocolo sería sometido a su aprobación, pero a la fecha todavía no se ha aprobado y además se cuestionó la base jurídica para el desarrollo de ese protocolo y eventuales lineamientos operativos para el manejo de crisis cibernéticas a nivel nacional.

139. En una de las sesiones virtuales también se indicó que la gestión de crisis cibernéticas es coordinada por el CNC, incluso ya han tenido reuniones específicas para coordinar el accionar ante crisis que implican un potencial riesgo para el país. Dicho lo anterior, las autoridades competentes, MINTEL, CNC, MDN, entre otros, deben definir la autoridad competente, aprobar el protocolo de gestión de crisis cibernéticas y dotar a la estructura de los recursos necesarios.

140. En las sesiones virtuales se determinó que no hay un programa nacional para la coordinación de simulacros (cyberdrills) ni una estructura coordinada para la comunicación de emergencias y/o crisis. Se desconoce si el borrador del protocolo arriba indicado establecía la organización de simulacros basados en diferentes escenarios cibernéticos y una estructura de comunicación de emergencias.

141. Según se informó en las sesiones virtuales, MINTEL, EcuCERT, MDN, COCIBER, etc. todavía no han organizado un simulacro a nivel nacional. Sin embargo, oficiales y funcionarios de dichas entidades han participado en simulacros domésticos, regionales e internacionales, lo cual implica que si existe recurso humano capacitado para la organización, coordinación y ejecución de este tipo de simulacros.

142. El MDN y el CIES están trabajando en la implementación de una plataforma para la realización de simulacros a nivel nacional, y se estima que para el último trimestre del año 2022 se organice un simulacro con actores de todos los sectores.

143. En la PNC se hace referencia al desarrollo de capacidades para hacerle frente a crisis cibernéticas, pero no se define como objetivo el desarrollo e implementación de un plan nacional de gestión de crisis. También se menciona la realización de dos tipos de ejercicios o simulacros, unos para evaluar la efectividad de los planes de contingencia, u otros para simular escenarios de crisis. Sin embargo, ambos simulacros tienen un enfoque limitado, ya que están orientados a mejorar las capacidades dentro de las infraestructuras críticas digitales (ICD), dejando por fuera otros actores que no forman parte de la comunidad de las ICD.

Este Factor estudia la capacidad del gobierno para identificar los activos de IC, los requisitos normativos específicos de la ciberseguridad de IC y la implementación de buenas prácticas de ciberseguridad por parte de los operadores de ICI.

D 1.3 PROTECCIÓN DE INFRAESTRUCTURAS CRITICAS (IC)

Nivel de Madurez: Formativo a Establecido

144. Ecuador no ha identificado formalmente los sectores, subsectores y activos de las infraestructuras críticas a nivel nacional.

145. De conformidad con la PNC, el Ministerio de Defensa Nacional (MDN) es la institución responsable de la protección de las infraestructuras críticas digitales y servicios esenciales en Ecuador (Pilar 3). Es importante señalar que, en la PNC no existe un apartado de definiciones generales, por lo que la definición y alcance de las "infraestructuras críticas digitales y servicios esenciales" no está claro.

146. En la PNC se indica que, en el año 2019, se desarrolló una guía para el levantamiento de las infraestructuras críticas, pero es hasta el año siguiente en que el MDN y el COCIBER, usando una metodología propia, iniciaron el proceso de identificación de las infraestructuras críticas en Ecuador. En dicho levantamiento participaron únicamente las instituciones públicas (telecomunicaciones, sector energético, sector financiero, etc.) y no se tomó en cuenta -nuevamente- a las empresas del sector privado, la cuales también ofrecen servicios críticos y esenciales en el país. Incluso, en varios sectores existen operadores privados que operadores públicos, por ejemplo, en el sector de telecomunicaciones, esto es debido a que el campo de acción según las atribuciones no incluye el sector privado.

147. Se indicó que la metodología utilizada establecía una serie de definiciones, marcos legales (sectores estratégicos), órganos ejecutores, taxonomía de infraestructuras críticas de la información, la cual pretendía identificar las infraestructuras y los activos críticos en el ámbito de Information Technology (IT) y Operational Technology (OT). La metodología también definía criterios de valoración basados en componentes de impacto al Producto Interno Bruto y aspectos sociales, económicos, medioambiente y políticos. Las instituciones que participaron del levantamiento completaron un documento matriz, evaluando todos esos factores, el cual fue entregado a MDN.

148. A la fecha, el MDN no ha publicado los resultados de ese levantamiento, pero en una de las sesiones virtuales un representante de gobierno se comprometió a darle seguimiento y coordinar con MINTEL y COCIBER los pasos a seguir para finalmente identificar las infraestructuras críticas digitales y servicios esenciales.

149. Durante las sesiones virtuales, un representante del sector público indicó que en su momento el MDN compartió una presentación donde se mostraban, según una matriz de riesgo y calor, cuáles sectores eran considerados como críticos. En varias sesiones también se comentó que posiblemente ese levantamiento está desactualizado y que es muy probable que MDN ocupe actualizar la información de ese levantamiento, así como determinar si la metodología usada realmente evalúa los componentes necesarios para identificar adecuadamente las infraestructuras críticas digitales de Ecuador. Por otro lado, varios participantes indicaron que proveedores de servicios

críticos del sector privado no fueron tomados en cuenta, lo cual implica que la metodología y alcance del levantamiento realizado por MDN no estaba alineado de los estándares y buenas prácticas internacionales en la materia, esto es debido a que el ámbito de acción y atribuciones del MDN es limitado.

150. Producto de ese levantamiento, MINTEL como ente rector del sector de telecomunicaciones, en conjunto con la ARCOTEL solicitaron a los operadores de telecomunicaciones, tanto públicos como privados, cierta información del inventario de los activos que internamente son catalogados como infraestructuras críticas. Lo anterior está fundamentado en la norma técnica 2018-0652, que entró en vigor en el año 2019. Esa norma técnica debe aplicarse de forma permanente por parte de los operadores y su aplicación es auditada por ARCOTEL anualmente. No existe evidencia de que ese tipo de normas regulatorias se hayan implementado en otros sectores.

151. Durante las sesiones virtuales se determinó que la gran mayoría los operadores y proveedores de servicios esenciales entienden y conocen su estatus -principalmente las transnacionales- y de que ofrecen servicios esenciales a la sociedad, los cuales en caso de disrupción podrían generar una conmoción social y económica. También se determinó que la gran mayoría de los operadores y proveedores consideran a la ciberseguridad como un tema prioritario para garantizar la seguridad de sus activos e infraestructura y la continuidad de la operación.

152. En una de las sesiones virtuales, representantes del sector aeroportuario manifestaron que a nivel gerencial existe un nivel de concientización alto en temas de ciberseguridad y que más bien son ellos lo que constantemente promueven la adopción de políticas, protocolos y herramientas de ciberseguridad y dotan de recursos a los departamentos de tecnología y ciberseguridad, pues entienden claramente el impacto adverso que podría generar al país la interrupción del servicio aeroportuario por un ataque cibernético.

153. En una de las sesiones virtuales, varios representantes de proveedores del sector energético manifestaron que en la parte técnica hace falta un mayor conocimiento sobre la ciberseguridad industrial. También se determinó que en el sector portuario el nivel de concienciación es todavía bajo y existe una carencia de recursos y personal capacitado para proteger la infraestructura y redes.

154. También se determinó en las sesiones virtuales que, un número menor de los operadores y proveedores de servicios esenciales han identificado y establecido los protocolos y las medidas de control para minimizar el impacto de las dependencias transfronterizas.

155. Tanto los operadores del sector de telecomunicaciones como las entidades del sector financiero, principalmente, están sujetas a resoluciones, directrices o normas técnicas sectoriales orientadas a fortalecer la postura de ciberseguridad mediante la implementación de lineamientos de seguridad basados en estándares internacionales. En esa línea, tanto MINTEL como la Superintendencia de Bancos han establecido los procedimientos para monitorear y auditar el cumplimiento de las resoluciones, directrices o normas técnicas sectoriales que fortalecen la ciberseguridad.

156. No obstante, esas resoluciones, directrices o normas técnicas sectoriales todavía no tienen un enfoque holístico. Una vez que se identifiquen y regulen los sectores críticos digitales y servicios esenciales, es muy probable que los reguladores sectoriales impongan mayores medidas y controles en materia de ciberseguridad para asegurarse que los servicios son suministrados de forma ininterrumpida. Ya la Superintendencia de Banco está trabajando en el fortalecimiento de las normas técnicas y el marco regulatorio en general a través, el MINTEL como ente rector de seguridad de la información se encuentra ejecutando memorandos de entendimiento

con organismos internacionales como CYBER4DEV y CYBERNET, para ejecutar acciones de fortalecimiento en el ámbito de la ciberseguridad.

157. En una de las sesiones virtuales, un representante del sector de telecomunicaciones indicó que el alcance de una norma técnica de ARCOTEL tiene un alto costo de cumplimiento y requiere mayor efectividad para mejorar la seguridad de los clientes, lo cual denota que los operadores cumplen con las normas técnicas existentes incluso cuando esas normas técnicas les generan una sobrecarga regulatoria y administrativa y un alto costo operativo.

158. El Ministerio de Energía, en su calidad de ente rector en el sector energético, todavía no emite normas técnicas sobre ciberseguridad sobre la base de que MINTEL es el ente competente de esos temas a través de la implementación del EGSI Versión 2.0; sin embargo, ese esquema aplica a las instituciones de la administración pública central dependiente de la función ejecutiva, entonces ¿qué sucede con las empresas privadas del sector energético?, ¿algún ente las supervisa o regula desde la óptica de la ciberseguridad? Por otro lado, la Dirección de Aviación Civil (DAC), como ente rector del sector aeroportuario, tampoco ha emitido normas técnicas o directrices en el ámbito de la ciberseguridad. Lo mismo sucede con el Ministerio de Salud como rector de los centros de salud y hospitales públicos. Tampoco el Ministerio de Transporte ha emitido directrices o normas técnicas al sector portuario en temas de ciberseguridad. Participantes del sector público indicaron que instituciones no pertenecientes a la Administración Pública toman el EGSI Versión 2.0 como una buena práctica.

159. La gran mayoría de los operadores y proveedores de servicios esenciales informaron que implementan estándares internacionales (e.g., ISO 27.001) y sectoriales (e.g., estándares del North American Electric Reliability Corporation (NERC) de seguridad como una buena práctica requerida por la casa matriz y/o la administración para garantizar la continuidad de la operación. Así mismo, en el sector financiero, las entidades reguladas deben cumplir adicionalmente con estándares que son requeridos por emisores de tarjetas (estándar PCI DSS). En una de las sesiones virtuales se indicó que, en el sector de aeroportuario, ya las autoridades internacionales de aviación están promoviendo e imponiendo regulaciones en el ámbito de la ciberseguridad.

160. Como se indicó en la sección de respuesta a incidentes (D1.2), en el universo de operadores y proveedores de servicios esenciales, solo los operadores de telecomunicaciones -tanto públicos como privados- tienen la obligación, según la norma técnica 2018-0652, de reportar los incidentes cibernéticos y divulgar las vulnerabilidades a ARCOTEL a través del EcuCERT. Lo mismo sucede en el sector financiero, se debe reportar a la Superintendencia de Banco los incidentes, en general, que interrumpan la disponibilidad del servicio. También se indicó que, tanto ARCOTEL a través del EcuCERT como la Superintendencia de Bancos no brindan soporte técnico a las entidades reguladas durante la etapa de recuperación, pero si se aseguran de que el servicio se restablezca; estas acciones las realizan cada institución según su Plan de Contingencia o Procesos de Gestión de Riesgos Cibernéticos establecidos.

161. Los operadores y proveedores de servicios esenciales obligados al cumplimiento del EGSI vo2 (control 12) deben reportar los incidentes a MINTEL. Dicho lo anterior, y así quedó en claro en las sesiones virtuales, que los proveedores de servicios esenciales del sector energético, puertos, aeropuertos, entre otros, no están obligados a reportar sus incidentes a la autoridad regulatoria, lo cual significa que en varios sectores críticos la ciberseguridad todavía no está completamente integrada en el ámbito regulatorio.

162. En el sector financiero, BanRed, una empresa privada proveedora de servicios financieros, tiene un comité de seguridad y además las entidades financieras que contratan sus servicios tienen la obligación de reportar los incidentes cibernéticos. Se desconoce si BanRed realiza

alguna gestión de seguimiento o si esos incidentes reportados son luego escalados a las autoridades competentes.

163. A los operadores y proveedores de servicios esenciales también les aplicaría las disposiciones de la Ley Orgánica de Protección de Datos en caso de darse una brecha de seguridad. Los artículos 43 y 46 establecen el procedimiento de notificación tanto de los reportes de brechas de seguridad como de las vulnerabilidades de seguridad.

164. Así mismo, no en todos los sectores de servicios esenciales se requiere la evaluación de riesgos cibernéticos como parte de las obligaciones regulatorias, pero la mayoría de los operadores y proveedores, como una buena práctica, si han integrado un análisis de riesgos cibernéticos dentro de sus actividades de gestión de riesgos. Por ejemplo, la Superintendencia de Bancos solicita evaluaciones de riesgos de forma periódica, pero los riesgos cibernéticos todavía no son parte del reporte de cumplimiento; sin embargo, las entidades financieras evalúan los riesgos cibernéticos como una buena práctica.

165. En varios sectores que brindan servicios esenciales, se está dando un intercambio de información sobre incidentes cibernéticos, vulnerabilidades, etc. mediante canales de comunicación formales e informales. Actualmente, la plataforma de intercambio de información más robusta en Ecuador es la RNC del EcuCERT, por lo que se debería incentivar su aplicación y ampliar la comunidad objetivo. Todavía hace falta fortalecer este tipo de iniciativas y los protocolos de confidencialidad a nivel sectorial -quizá coordinados por un ente de coordinación sectorial o nacional, generando la normativa que permita realizar estas acciones.

166. A nivel sectorial, en Ecuador se han realizado pocos simulacros (cyberdrills) y en algunos sectores específicos. En el año 2016, ARCOTEL en colaboración con la Escuela Politécnica Nacional organizaron un evento denominado "la semana de la ciberseguridad desde la mitad del mundo" y donde se realizaron varias actividades, entre ellas, un simulacro sectorial. Desde entonces, ARCOTEL no ha organizado más simulacros en el sector de telecomunicaciones por temas presupuestarios. En el sector aeroportuario, el Consejo Internacional de Aeropuertos (ACI por sus siglas en inglés - Airports Council International y su filial ACI-LAC (su oficina para América Latina y el Caribe) organizaron un simulacro donde participaron varios aeropuertos internacionales y se simuló un ataque cibernético en un aeropuerto ficticio.

167. Hasta que los temas mencionados anteriormente se fortalezcan, incluida la identificación oficial de los sectores y activos de infraestructuras críticas, un marco formal de notificación de incidentes, el desarrollo de un marco regulatorio robusto de protección de infraestructuras críticas e incentivos reales para cumplir con dicho marco regulatorio es poco probable que el Gobierno sea capaz de garantizar de que los activos de infraestructura crítica en el país están adecuadamente protegidos.

D 1.4 CIBERSEGURIDAD EN LA DEFENSA Y SEGURIDAD NACIONAL

Este Factor evalúa si el gobierno tiene la capacidad para diseñar e implementar una estrategia de ciberseguridad dentro de las estructuras de defensa y seguridad nacional, y el nivel de capacidad de ciberseguridad de esas estructuras, así como los acuerdos de colaboración en ciberseguridad entre las entidades civiles y de defensa.

Nivel de Madurez: Establecido

168. El Ministerio de Defensa Nacional (MDN) es el ente rector de la Defensa a nivel nacional, lo cual incluye las operaciones de ciberdefensa. El MDN entiende, en todas sus estructuras, la importancia de tomar medidas estratégicas orientadas a la protección de las infraestructuras críticas y de la soberanía en general, así como la identificación y contención de las amenazas y ataques cibernéticos que ponen en riesgo la estabilidad política, social y económica del país. Lo anterior está expresamente reconocido y estipulado en la Política de Defensa Nacional del 2018 (PDN), la cual también mencionó la necesidad de desarrollar una estrategia de ciberdefensa debido a que las estructuras de defensa y seguridad nacional dependen en gran medida del uso de las tecnologías de la información y comunicación (TICs) y otras infraestructuras críticas digitales.

169. De conformidad con la PNC, el MDN es la autoridad responsable del Pilar 4, el cual abarca el tema de soberanía y ciberdefensa a nivel nacional, y del Pilar 3, el cual se enfoca en el tema de protección a las infraestructuras críticas digitales y servicios esenciales. Sin embargo, la PNC es omisa en cuando a los objetivos y líneas de acción relacionadas con el Pilar 4, ya que no se especifica qué acciones deberá liderar e implementar el MDN en el ámbito de la ciberdefensa.

170. Basado en los objetivos estratégicos de la PDN, en el año 2021 el MDN adoptó la Estrategia de Ciberdefensa, cuyo propósito es el fortalecimiento de la ciberdefensa como una capacidad necesaria para el cumplimiento de la misión constitucional de la defensa y además para desarrollar las capacidades para realizar operaciones de defensa, exploración y respuesta a los efectos producidos por los ciberataques, asegurando una defensa efectiva de las infraestructuras digitales. En una de las sesiones virtuales se indicó que, también existe una estrategia de ciber inteligencia, pero es documento reservado.

171. El MDN está trabajando para que sus operaciones en el ciberespacio y cualquier otra actividad en el ámbito de la ciberdefensa, incluyendo las políticas y estrategias arriba indicadas, estén alineadas al derecho internacional humanitario y las buenas prácticas internacionales.

172. En una de las sesiones virtuales se indicó que, en el MND, a través del Comando de Ciberdefensa (COCIBER), se realizan evaluaciones de los riesgos cibernéticos, mensualmente o cuando se requieran, para identificar las amenazas a las que está expuesto el país. Los resultados de esas evaluaciones son documentos reservados y confidenciales y no fueron utilizados como insumo durante el desarrollo de la Estrategia de Ciberdefensa y/o de la PNC.

173. Se indicó que El COCIBER es el comando de ciberdefensa creado en el año 2014, cuya misión es realizar operaciones militares de defensa, exploración, y amenazas, que son ejecutadas de forma permanente para proteger la infraestructura de las Fuerzas Armadas y del Estado, y también ejecutar operaciones de respuesta.

174. Dentro del COCIBER, se creó un CERT militar, el cual es reconocido como tal por la Organización de los Estados Americanos. Así mismo, el COCIBER están tramitando la certificación ante FIRST en colaboración tanto del EcuCERT como de CERT CEDIA (Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia).

175. El CERT militar del COCIBER realiza las actividades de gestión de incidentes, análisis de vulnerabilidades, análisis de malware en dispositivos celulares, y también hacen test de penetración, hackeo ético, entre otros. En cuanto a las operaciones militares, se hacen por defensa y exploración con enlace y respuesta.

176. Dicho CERT militar tiene un staff de 5 oficiales con las competencias adecuadas; sin embargo, en situaciones críticas o de crisis se han convocado más oficiales, incluso se ha llegado a operar con un staff de 30/35 oficiales. Todos esos oficiales tienen formación en el área de informática, algunos con mayor experiencia y atestados que otros, pero en general se debe mejorar el nivel de capacitación y formación. El COCIBER tiene una política interna de capacitación, pero no se cumple debido a la falta de recursos financieros y disponibilidad de cursos especializados. La mayoría de los cursos y capacitaciones se hacen de forma virtual con la colaboración de socios internacionales -Colombia u otros países de la región.

177. En las sesiones virtuales se determinó que, COCIBER requiere de más recursos, pues tanto las amenazas como las infraestructuras TIC en el sector militar han crecido sustancialmente. Se está planeando la creación de un SOC militar, pero primero tienen que resolver el tema de los recursos financieros. Actualmente, el COCIBER está gestionando la contratación de más recursos humano capacitado, no obstante, la carencia de expertos con la formación y capacitación adecuada se ha convertido en una limitante.

178. También se indicó que, en el año 2022 se tiene planeado realizar una inversión importante para mejorar las capacidades operativas del COCIBER. En esa línea, se está abriendo un curso de Ciberdefensa, del cual se espera con-

tratar un contingente con habilidades técnicas y militares y que además hayan superado los filtros de seguridad correspondientes para asegurar un personal técnico confiable.

179. Se informó que, el COCIBER ha establecido mecanismos de cooperación con varios socios estratégicos en el tema de capacitación de su personal, entre ellos, MINTEL, pares militares, Foro Interamericano de Ciberdefensa (FIC), etc., pero se deben crear más y mejores opciones de capacitación para su personal.

180. Se mencionó que dos de los desafíos del COCIBER son, primero, el tema de presupuesto para cumplir con cada una de las tareas y objetivos asignados, y segundo, la carrera militar, reclutamiento y retención de personal, ya que existe mucha rotación de personal dentro de la estructura de defensa.

181. Aunque la protección de las infraestructuras críticas digitales y servicios esenciales es parte de las obligaciones del MDN, todavía no se implementan actividades orientadas al monitoreo y protección de estas a nivel nacional. Sin embargo, el MDN recientemente solicitó el acompañamiento de MINTEL para iniciar formalmente con esas funciones que le fueron delegadas en la PNC.

182. El COCIBER está constantemente monitoreando temas de hacktivismo e información falsa en redes sociales, ya que representan una amenaza a la estabilidad del país. Recientemente, el COCIBER identificó un grupo global de hackactivistas que estaba usando las redes sociales para alterar el orden en Ecuador u otros Estados de la región por medio de noticias falsas y campañas de desinformación con fines políticos y de salud (pandemia). Esas operaciones de influencia fueron identificadas y se está analizando la situación y la forma de cómo abordarla.

183. El COCIBER trabaja muy de cerca con el EcuCERT y es parte de la RNC, donde se comparte información a través de varios medios, como aplicaciones de mensajería instantánea, correo electrónico, y ahora se está en el proceso de implementar la plataforma MISP (Malware Information Sharing Platform) con el apoyo del EcuCERT.

184. También el MDN y el COCIBER tienen una buena relación con CIES y la Policía Nacional en temas de inteligencia y la lucha contra el cibercrimen, pero todavía no han establecido canales de comunicación con agencias de cumplimiento de la ley regionales o internacionales.

185. MDN es miembro del FIC, cuyo objetivo es promover la cooperación regional para afrontar juntos los retos que se presentan en el ciberespacio y así contrarrestar las amenazas que atentan contra la seguridad nacional de los estados miembros -Argentina, Brasil, Chile, Colombia, España, México, Paraguay, Perú, Portugal, Uruguay y Ecuador.

186. En el FIC se han establecido mecanismos de cooperación entre sus miembros, que incluyen el intercambio de información y experiencias, a través de canales formales e informales, así como el desarrollo de capacidades humanas, a través de ofertas educativas y la organización de ejercicios o simulacros (cyberdrills). El rol del MDN y el COCIBER dentro de FIC es relativamente activo, participan en conferencias, capacitaciones u otros eventos académicos, en los boletines semanales, etc. En el año 2021, varios oficiales del COCIBER participaron en un cyberdrill celebrado en Colombia, el cual fue organizado por las fuerzas militares colombianas y participaron 12 países. En ese evento el COCIBER obtuvo el segundo lugar en la competencia.

RECOMENDACIONES

187. Las siguientes recomendaciones están basadas en los indicadores de la metodología del CMM, así como en los aportes o sugerencias de los participantes. El equipo de investigación también realiza recomendaciones basadas en buenas prácticas que aplican en otros países.

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

R1.1 Durante el proceso de actualización de la PNC, se recomienda tomar en consideración las siguientes acciones:

1. Realizar una evaluación nacional de riesgos cibernéticos para garantizar que el contenido de la PNC y su plan de acción estén alineados con las prioridades y necesidad actuales para responder al entorno cambiante.
2. Hacer un levantamiento de los socios estratégicos en el sector privado, sector académico, sociedad civil, u otros actores no gubernamentales.
3. Incentivar la participación de esos socios estratégicos en los talleres, evaluaciones, grupos de trabajo y/o proceso de consulta pública, así como considerar sus comentarios, sugerencias e iniciativas durante el proceso de desarrollo y revisión de las políticas públicas en el ámbito de la ciberseguridad -incluyendo la PNC y su plan de acción.
4. Asegurarse que las políticas públicas en el ámbito de la ciberseguridad -incluyendo la PNC y su plan de acción- tengan un enfoque y alcance holístico y que contemplen líneas de acción que reflejen las necesidades y prioridades a nivel nacional. Asimismo, que esas políticas públicas tengan un vínculo directo con otras políticas y estrategias nacionales en el ámbito social y económico.
5. Asegurarse que la PNC y su plan de acción tienen líneas de acción robustas y abarcan los siguientes temas: protección a la niñez en línea, promoción y respeto de los derechos humanos, promoción de la igualdad, diversidad e inclusión, y un tema muy importante, la gestión de noticias falsas o prácticas de desinformación. Así mismo, que promuevan el establecimiento de alianzas público-privadas y campañas nacionales de concientización.
6. Asegurarse que la PNC y su plan de acción contemplen un programa (detallado) de monitoreo y revisión (también denominado de seguimiento y evaluación), que incluya el registro de métricas y estadísticas sobre la efectividad del proceso de implementación y la remisión periódica de informes a las autoridades competentes. Así mismo, que esas métricas sean revisadas periódicamente y que informen los procesos de toma de decisiones y la asignación de recursos.
7. Monitorear y evaluar las funciones y responsabilidades de los ministerios y entidades públicas a cargo de los pilares de la PNC, lo cual incluye identificación de brechas, duplicidad de funciones y falta de recursos.
8. Considerar la creación de un Programa Nacional de Ciberseguridad que tenga objetivos y metas claras y un presupuesto adecuado, y que además tenga los siguientes componentes:
   8.1. Una estructura de gobernanza de ciberseguridad con mandatos legales, funciones y responsabilidades debidamente establecidas y que todo el ecosistema, incluido el público en general, comprenda esa estructura y la forma de cómo los riesgos y los inciden-

tes cibernéticos u otros problemas se escalan a los niveles más altos del Gobierno.

8.2 Un coordinador nacional de ciberseguridad (NCC) con mandato legal para liderar el Programa Nacional de Ciberseguridad, y que además tenga la autoridad para consultar e interactuar con representantes de los sectores público y privado, la academia y la sociedad civil. El NCC podría ser una agencia dentro de un ministerio o cualquier otra entidad gubernamental, pero se recomienda que sea un ente independiente y con recursos suficientes.

9. Asegurarse que la PNC y su plan de acción estén alineados con otras prioridades, estrategias y planes nacionales para evitar la duplicidad de esfuerzos y mal uso de recursos.
10. Implementar estándares y buenas prácticas en el proceso de desarrollo y revisión de políticas públicas (incluyendo la PNC y su plan de acción), específicamente en aquellas orientadas a desarrollar una estrategia nacional de seguridad cibernética. Consultar la "Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad" desarrollada por la UIT, el Banco Mundial y otras organizaciones internacionales.

R1.2 Durante el proceso de implementación de la PNC y su plan de acción, se recomienda tomar en consideración las siguientes acciones:

1. Asegurarse que el plan de acción defina (en detalle) las líneas de acción y actividades específicas, entidades responsables, recursos, presupuesto y fechas de entrega, y que además involucre a todos los actores del ecosistema, incluyendo entidades públicas y privadas, academia, sociedad civil, entre otros.
2. Asegurarse que las autoridades competentes asignen un presupuesto razonable para financiar tanto el proceso de revisión como de implementación de la PNC y su plan de acción. Así mismo, realizar periódicamente auditorías a las provisiones presupuestarias para escalar los resultados y preocupaciones a nivel ministerial para su resolución.
3. Promover la creación de alianzas público-privadas, para que organizaciones no gubernamentales participen y asuman un papel más preponderante en el proceso de implementación de la PNC y su plan de acción.
4. Realizar periódicamente una evaluación integral para determinar de qué forma se afectan tanto los intereses del país como su posicionamiento a nivel global en los debates internacionales sobre políticas de ciberseguridad.

RESPUESTA A INCIDENTES Y GESTIÓN DE CRISIS

R1.3 Evaluar tanto el mandato legal, capital humano, recursos y equipo tecnológico, como los procedimientos operativos y el desempeño en general del EcuCERT (o del CSIRT que se le deleguen las funciones y responsabilidades de CERT nacional), para luego implementar las acciones que sean necesarias con el fin para garantizar que, en un periodo razonable, el EcuCERT opere como el centro nacional de respuesta a incidentes de Ecuador.

R1.4 Asegurarse que el EcuCERT (o el CSIRT que se le deleguen las funciones y responsabilidades de CERT nacional) registre todos los incidentes cibernéticos a nivel nacional y que además cuenta con los procedimientos para el escalamiento de los incidentes, desde un nivel organizacional a nivel nacional. Así mismo, una vez categorizados los incidentes de conformidad con los niveles de criticidad, existe la capacidad de asignarse los recursos según las necesidades.

R1.5 Establecer una estrategia de capacitaciones para los empleados del EcuCERT (o del CSIRT que se le deleguen las funciones y responsabilidades de CERT nacional), con recursos económicos suficientes, y definir métricas para evaluar los resultados de esas capacitaciones.

R1.6 Gestionar los recursos necesarios para la actualización de las herramientas y equipo tecnológico -software y hardware- y así contar con los recursos idóneos en la gestión del ciclo de respuesta a incidentes.

R1.7 Considerar la elaboración e implementación de un marco nacional de notificación de incidentes cibernéticos, que obligue a todas las instituciones de los sectores público y privado, incluidos los operadores de IC y servicios esenciales, a informar, de manera oportuna, los incidentes cibernéticos al EcuCERT (o al CSIRT que se le deleguen las funciones y responsabilidades de CERT nacional) u otras autoridades competentes.

R1.8 Considerar la elaboración e implementación de un marco y/o plataforma nacional para el intercambio de información relacionada con incidentes cibernéticos, vulnerabilidades y otras medidas preventivas. Así mismo, esa plataforma deberá contar con protocolos formales de confidencialidad y ampliar la comunidad objetivo incluso a socios internacionales.

R1.9 Fortalecer las capacidades y mecanismos internos de gestión de incidentes de las instituciones públicas y privadas, lo cual incluye los protocolos para la identificación, contención y resolución de los incidentes cibernéticos.

R1.10 Fortalecer los actuales convenios, acuerdos y mecanismos de cooperación regional e internacional para resolver los incidentes cibernéticos conforme ocurran.

R1.11 Proporcionar suficientes recursos al EcuCERT (o al CSIRT que se le deleguen las funciones y responsabilidades de CERT nacional) para fortalecer la organización e implementación de programas nacionales de concientización.

R1.12 Considerar la elaboración e implementación de un plan nacional de gestión de crisis, en el cual la ciberseguridad deberá ser un componente importante dentro de la estructura, protocolos y planificación. Además, asegurarse de designar a un ente responsable para la gestión de crisis, con funciones y responsabilidades claras y que además esté equipado (mandato, recursos, capital humano) para gestionar diferentes escenarios de ataques cibernéticos.

R1.13 Implementar un programa nacional de simulacros (cyberdrills) -con suficientes recursos y donde participen todos los actores relevantes del ecosistema. Así mismo, definir métricas y estadísticas para evaluar los resultados de esos ejercicios y que además informen los procesos de toma de decisiones y asignación de presupuesto.

R1.14 Asegurarse que el sistema nacional de comunicación de emergencias es probado periódicamente para medir su nivel de resiliencia cibernética ante diferentes escenarios de ataques cibernéticos.

PROTECCIÓN A LAS INFRAESTRUCTURAS CRÍTICAS (IC)

R1.15 Realizar la evaluación nacional de riesgos cibernéticos (ver recomendación R1.1.1) a efectos de identificar las infraestructuras críticas digitales y servicios esenciales a nivel nacional, así como determinar los niveles de criticidad y dependencias e interdependencias.

R1.16 Asegurarse que los proveedores y operadores de servicios esenciales, tanto públicos como privados, participen en esa evaluación -y en las futuras actualizaciones.

R1.17 Asegurarse de formalizar y difundir la lista oficial de los sectores de infraestructuras críticas digitales y servicios esenciales. Así mismo, realizar estas evaluaciones de forma periódica para mantener actualizada la lista indicada anteriormente.

R1.18 Desarrollar e implementar un marco regulatorio de protección a las infraestructuras críticas con el fin de obligar a los operadores y proveedores a cumplir con estándares técnicos y legales específicos, tales como la implementación de estándares de seguridad reconocidos internacionalmente, requisitos de reporte de incidentes, evaluaciones y gestión de riesgos, requisitos de seguridad con respecto a la cadena de suministro, prácticas de divulgación responsable de vulnerabilidades, mecanismos de intercambio de información, etc. Lo anterior para garantizar que los operadores y proveedores están protegiendo adecuadamente los sectores, subsectores y activos catalogados como infraestructuras críticas digitales y servicios esenciales.

R1.19 Establecer el modelo de gobernanza en el ámbito de la protección a las infraestructuras críticas digitales y servicios esenciales, lo cual implica que se determine cuáles agencias gubernamentales y/o reguladores sectoriales serán responsable de monitorear y hacer cumplir el marco regulatorio antes indicado, y además se definan sus funciones y responsabilidades. Asimismo, asegurarse que esas autoridades regulatorias cuentan con los recursos suficientes para cumplir su mandato.

R1.20 Aunque todavía no están identificadas las IC ni existe un marco regulatorio, los proveedores y operadores de servicios esenciales al menos podrían considerar implementar las siguientes acciones como una buena práctica:

1. Implementar, y auditar periódicamente, estándares internacionales y mejores prácticas de seguridad, y controles y protocolos de ciberseguridad industrial.
2. Realizar auditorías periódicamente para evaluar las dependencias, interdependencias y vulnerabilidades de la red y el sistema para informar la reevaluación continua de la cartera de riesgos, tecnologías, políticas y procesos de IC.
3. Implementar y monitorear la evaluación y los procesos de gestión de riesgos cibernéticos respaldados por soluciones técnicas de seguridad, enlaces de comunicaciones y medidas de mitigación.
4. Asegurarse de que los proveedores y operados de IC, tanto públicos como privados, tengan en modo operativo las capacidades técnicas, recursos y protocolos de prevención, detección y respuesta a incidentes.
5. Establecer acciones formales e informales para incentivar la coordinación y el intercambio de información entre los actores relevantes del ecosistema de IC. Además, fomentar la confianza entre el gobierno y los operadores de IC en materia de ciberseguridad e intercambio de información sobre vulnerabilidades, incidentes y amenazas.
6. Realizar periódicamente actividades de capacitación internas para que los miembros de la administración puedan entender los mecanismos de inteligencia del riesgo cibernético, gestionar crisis y participar en la gestión de riesgos y los procesos de respuesta a incidentes de manera general. Y que esas actividades de capacitación también se extiendan al resto del personal.
7. Asignar recursos suficientes, de conformidad con el impacto evaluado del incidente, para garantizar una respuesta rápida y eficaz al incidente.

CIBERSEGURIDAD EN LA DEFENSA Y SEGURIDAD NACIONAL

R1.21 Evaluar la necesidad de revisar y actualizar la Estrategia de Ciberdefensa 2021, siempre que los cambios realizados a la PNC generen un impacto importante en sus objetivos y líneas de acción.

R1.22 Asegurarse que el MDN, a través del COCIBER, tiene las capacidades para cumplir las funciones delegadas tanto por la PNC y su plan de acción, como por la Estrategia de Ciberdefensa 2021, principalmente la función de monitoreo y protección a las infraestructuras críticas digitales y servicios esenciales.

R1.23 Realizar simulacros periódicamente dentro de las estructuras militares para evaluar las capacidades, estructuras organizacionales, procedimientos y recursos. Así mismo, definir métricas y estadísticas para evaluar los resultados de esos ejercicios y que además informen los procesos de toma de decisiones y asignación de presupuesto.

R1.24 Asegurarse de que el CERT militar cuenta con los recursos tecnológicos y financieros y capital humano para realizar las operaciones de ciberdefensa y otras funciones delegadas. Así mismo, asegurarse que su personal sea capacitado periódicamente según la estrategia de capacitaciones.

R1.25 También implementar recursos de inteligencia especializados para brindar apoyo a las operaciones de ciberdefensa y que además esas actividades cuentan con los recursos necesarios.

DIMENSION 2

CULTURA CIBERNÉTICA Y SOCIEDAD

188. Esta Dimensión evalúa elementos importantes de una cultura de ciberseguridad responsable, tales como la comprensión de los riesgos cibernéticos en la sociedad, el nivel de confianza en los servicios de Internet, gobierno electrónico y comercio electrónico, y la comprensión de los usuarios sobre la protección de los datos personales en línea. Además, esta Dimensión revisa la existencia y disponibilidad de mecanismos de denuncia para que el público en general denuncie los delitos informáticos. Además, esta Dimensión revisa el papel de los medios de comunicación y las redes sociales en la formación de valores, actitudes y comportamientos de ciberseguridad.

Este factor evalúa el grado en que la ciberseguridad se prioriza y se integra en los valores, actitudes y prácticas del gobierno, el sector privado y los usuarios de la sociedad en general. Así mismo, una buena mentalidad de ciberseguridad consiste en desarrollar una serie de valores, actitudes y prácticas -incluidos los hábitos de los usuarios, expertos y otros actores- que permiten aumentar el conocimiento y la capacidad de los usuarios para protegerse cuando están línea.

D 2.1 MENTALIDAD DE CIBERSEGURIDAD

Nivel de Madurez: Formativo a Establecido

189. Durante el presente diagnóstico se determinó que, el nivel de conciencia y conocimiento sobre los problemas y riesgos de ciberseguridad en Ecuador va en crecimiento, pero todavía no alcanza un nivel adecuado en términos generales. Sin embargo, cuando se analizan tanto grupos de actores y sectores específicos como el público en general, se identifica que hay varios niveles de conocimiento con respecto a los riesgos cibernéticos u otros temas relevantes de la ciberseguridad.

190. En el sector público, se observa que el nivel de conciencia sobre los riesgos cibernéticos en la mayoría de las instituciones públicas todavía es básico, pero factores como la implementación del EGSI Versión 2.0 en las instituciones de la administración pública central y los crecientes ataques cibernéticos a instituciones públicas en Ecuador hacen que la postura de ciberseguridad mejore paulatinamente y se comiencen a invertir más recursos en tecnología y capacitación del personal.

191. En la PNC, específicamente en el Pilar 7, se reconoce la necesidad de construir una cultura de ciberseguridad en todos los sectores, incluyendo al sector público. En este ámbito es muy importante el liderazgo que pueda tomar MINTEL y el EcuCERT, específicamente en la organización de campañas de concientización a nivel nacional y en especial para los funcionarios y servidores públicos.

192. También se determinó que algunas instituciones públicas realizan actividades de capacitación de forma esporádicas, pero no como parte de un programa de capacitación obligatorio para los funcionarios y servidores públicos. Tampoco existe algún tipo de inducción sobre ciberseguridad para los empleados nuevos en el gobierno o al menos una sesión informativa sobre las políticas y buenas prácticas que se aplican en el ámbito de la ciberseguridad. El EGSI Versión 2.0 fomenta, entre otros temas, que los funcionarios y servidores públicos deben capacitarse regularmente, pero para lograr un nivel óptimo, esas capacitaciones deben ejecutarse de forma regular y coordinada, lo cual todavía no se logra.

193. Posiblemente, el nivel de conciencia de las instituciones que cumplen con el EGSI Versión 2.0 es más avanzado que el nivel de conciencia que pueden tener los funcionarios de las entidades que no lo implementan y de

los gobiernos locales o municipalidades, así que esas instituciones también deben mapearse y formar parte de las políticas públicas de ciberseguridad en Ecuador.

194. En el sector privado el nivel de conciencia depende en gran medida del sector o industria y del tamaño de la empresa. Dentro de las empresas grandes o transnacionales, especialmente aquellas empresas que ofrecen servicios financieros, tecnológicos y/o telecomunicaciones, los funcionarios tienen un nivel de conciencia medianamente alto, ya que operan en sectores regulados y regularmente reciben capacitaciones, además de que la misma operación requiere que todos sus empleados tengan un nivel de conciencia adecuado para garantizar la disponibilidad del servicio.

195. En el sector de las PYMES, el nivel de conciencia puede variar, pero la mayoría de las PYMES realmente no consideran los riesgos cibernéticos como un tema prioritario hasta que ocurre un incidente que las afecte directamente. Sin embargo, el segmento de las PYMES poco a poco va aumentando el nivel de conciencia, pues en una de las sesiones virtuales se indicó que, varios proveedores de servicios de ciberseguridad ofrecen servicios y consultorías a las PYMES y que su cartera de clientes va en crecimiento -eso solo sucede únicamente cuando el nivel de conciencia también crece.

196. Con respecto a los usuarios de Internet se determinó que, en términos generales, estos tienen un nivel de conciencia limitado, pero existen factores como el ambiente laboral, grado de escolaridad, etc. que hacen que el nivel de conciencia mejore sustancialmente en ciertos sectores de la población. Para mejorar el nivel de conciencia de la población en general se debe capacitar a la ciudadanía desde la educación básica, es importante incluir en las mallas curriculares de los programas de educación formal, tanto de primaria como de secundaria, cursos con componentes de ciberseguridad y también implementar campañas de concientización dirigidos a sectores vulnerables, como la niñez, adultos mayores, mujeres jefas de hogar, etc. También se determinó que el sector financiero y la Policía Nacional cumplen un rol fundamental en la generación de conciencia mediante actividades, boletines informativos y/o pastillas en medios de comunicación masiva o redes sociales.

197. También se determinó que tanto los principales ministerios, agencias de gobierno e instituciones públicas como las principales empresas del sector privado implementan prácticas seguras de ciberseguridad. Así mismo, que un número limitado, pero creciente, de usuarios de Internet conocen o usan prácticas seguras de ciberseguridad. También se determinó que un número considerable de usuarios de Internet no utilizan del todo prácticas seguras de ciberseguridad.

Este Factor evalúa las habilidades críticas, la gestión de la desinformación, el nivel de confianza y creencia de los usuarios en el uso de los servicios en línea en general, y de los servicios de gobierno electrónico y comercio electrónico en particular.

D 2.2 CONFIANZA Y CREENCIA EN LOS SERVICIOS EN LINEA

Nivel de Madurez: Formativo a Establecido

198. Los participantes del presente diagnóstico consideran que solo un grupo limitado de usuarios de Internet realmente evalúan de forma crítica la información que ven y reciben por medios digitales. También se indicó que un grupo limitado de usuarios creen tener el conocimiento y capacidad para usar Internet de forma segura y también es limitado el grupo de usuarios que confía en el uso que le está dando al Internet.

199. También indicaron que en Ecuador no existen evaluaciones o métricas a nivel nacional que determinen el nivel de confianza que tienen los usuarios de Internet en la información que ven y reciben por medios digitales, como búsquedas en Internet (Google), redes sociales (Facebook, Instagram, Twitter), y otras aplicaciones (WhatsApp), etc.

200. Lo anterior es un tema que ha sido identificado por las autoridades competentes e incluso organizaciones del sector privado, académico y sociedad civil. Por tal motivo, se han desarrollado varios programas de alfabetización digital, entre ellos, los implementados en su momento por el Gobierno en los Infocentros y que ahora se llaman Puntos de Encuentro, donde también existen cursos de alfabetización digital más integrales basados en las guías temáticas del PLANADI (Programa Nacional de Alistamiento Digital).

201. También MINTEL, en colaboración con otras entidades, desarrolló una aplicación denominada "habilidades digitales", cuyo objetivo es medir las habilidades digitales de las personas en 5 áreas competenciales específicas, tales como información y alfabetización informacional, comunicaciones y colaboración, creación de contenidos digitales, seguridad de la información y resolución de problemas. Esta aplicación se ha usado en los más de 850 Infocentros Comunitarios del país. El programa "Internet para todos" implementado por MINTEL en donde se habían habilitado una o varias unidades móviles, con computadoras e Internet, en donde se impartían clases de alfabetización digital (de 40 min.) a los ciudadanos de las zonas rurales. Sin embargo, este programa ya no está en funcionamiento.

202. El MINTEL también desarrolla programas y mecanismos de alfabetización digital para toda la población, para asegurar niveles mayores y progresivos de aprovechamiento eficiente de las TIC. En ese sentido, desde el año 2012 hasta enero de 2021, el MINTEL alfabetizó digitalmente a 1.321.714 ciudadanos, priorizando las zonas rurales y urbano marginales.

203. También se mencionaron varias actividades virtuales organizadas por el Ministerio de Educación, tales como el programa denominado "Alfabetización Digital y Desinformación". Este programa fue implementando en el año 2021 y tiene como objetivo fomentar el pensamiento crítico, para tener una ciudadanía activa, responsable, pensante y participativa.

204. Así mismo, en la Agenda Digital Ecuador 2021-2022, específicamente en el eje Cultura e Inclusión Digital, existe un componente robusto de alfabetización digital, que busca asegurar la educación básica e inclusión social para que sectores vulnerables se incorporen al mundo digital.

205. La consultora internacional, The Economist Intelligence Unit, anualmente publica un Índice de Internet Inclusivo, el cual mide la penetración del servicio de Internet en 120 países (tipo ranking), entre ellos Ecuador, y en esa medición se evalúan cuatro factores: disponibilidad, asequibilidad, relevancia y preparación. En el ranking del 2021, Ecuador se encuentra posicionado en el puesto 81 en el factor de preparación (readiness), debido a que obtuvo una puntuación baja en el componente de confianza y seguridad, el cual evalúa la seguridad y la aceptación cultural del Internet. El factor de preparación también evalúa dos componentes más, la alfabetización (nivel de educación y preparación para usar el Internet) y las políticas públicas (la existencia de políticas nacionales que promueven la seguridad y el uso generalizado del Internet).

206. En el año 2020, la Universidad de Oxford publicó el reporte "Desinformación Industrializada, Inventario Global (2020) de la Manipulación Organizada de Redes

Sociales", en donde se destacan las principales tendencias de propaganda computacional usadas para manipular la opinión pública a nivel mundial. En el reporte se identificaron 81 países, entre ellos Ecuador, los cuales utilizan "cyber troop" o tropas cibernéticas en redes sociales para difundir propaganda y desinformación con fines políticos. Se indicó que Ecuador es víctima de tropas cibernéticas domésticas y de otros países de la región (e.g., Estraterra de Canadá) y cuya motivación es variada, algunas campañas de propaganda son pro-gobierno y también atacan a la oposición, otras son distractoras y otras son opresoras.

207. Debido al impacto negativo de las noticias falsas en temas específicos, la pandemia y el recién concluido proceso electoral, tanto MINTEL como el Consejo Nacional Electoral (CNE) han duplicado esfuerzos para combatir la desinformación o noticias falsas que circulan en redes sociales y otras plataformas digitales. En las pasadas elecciones, el CNE habilitó un canal de transmisión en vivo, la aplicación "CNE app", la asistencia de los medios de comunicación y las organizaciones políticas en el centro de mando y cadenas nacionales regulares, fueron estrategias claves para combatir las noticias falsa durante el proceso electoral. Un tema importante es que en Ecuador no reporta bloqueos sistemáticos o la filtración o censura de contenido por parte de las autoridades de gobierno.

208. El MINTEL también viene trabajando en varias campañas en diferentes medios de comunicación y redes sociales en donde se recomienda a los ciudadanos corroborar la información por medio de sitios oficiales y noticias confiables y se invita a tomar mayor atención a los mensajes que luzcan diferentes, ya que los archivos de imagen, video y audio pueden ser editados para intentar tergiversar la información.

209. Según el Instituto Nacional de Estadísticas y Censo, las aplicaciones de Facebook y WhatsApp son los principales canales de difusión de noticias falsas y campañas de desinformación en el país; sin embargo, en el reporte de la Universidad de Oxford se indicó que en el año 2020 la empresa Facebook eliminó varias cuentas y páginas tanto en Facebook como en Instagram que eran usadas para causar caos en Ecuador u otros países.

210. Se informó que desde la socieda
d civil también se realizan actividades para mitigar el impacto de las noticias falsas. Por ejemplo, en el año 2021 la coalición Ecuador Verifica (conformada por 18 medios de comunicación, 9 organizaciones de la sociedad civil y 7 universidades) organizó una conferencia para combatir la desinformación y las noticias falsas durante las elecciones presidenciales en Ecuador.

211. En Ecuador se ha identificado el impacto negativo que generan las noticias falsas y las campañas de desinformación, las cuales amenazan la estabilidad económica, social e incluso la democracia y seguridad nacional, por lo que es recomendable que en la revisión de la PNC se contemple una línea de acciones orientada a evaluar y establecer políticas públicas y mecanismos legales para contener este tipo amenazas en el país. Lo anterior se logra mediante acciones coordinadas y la participación de los actores clave del ecosistema.

212. En el presente diagnóstico se determinó que, el Gobierno de Ecuador ha puesto a disposición de la ciudadanía una gran variedad de servicios de gobierno electrónico, los cuales se encuentran disponibles en el siguiente portal web https://www.gob.ec. Dichos servicios van desde páginas meramente informativas hasta plataformas para realizar gestiones y pago de tributos, compras públicas, firma digital, constitución de empresas, ventanilla digital de trámites, entre otras gestiones. Incluso durante el inicio de la pandemia se implementó el servicio de emisión del certificado de defunción digital debido a la gran cantidad de fallecimientos que se dieron en la provincia de Guayas. Actualmente, el 60 % de los trámites están digitalizados, y el objetivo es que el 100 % de los trámites estén totalmente en línea a finales del 2022.

213. Según una encuesta realizada por el Banco Interamericano de Desarrollo (BID) en varios países de la región, se determinó que, en Ecuador existen todavía varios

Este Factor evalúa si los usuarios de Internet y las partes interesadas en los sectores público y privado reconocen y comprenden la importancia de proteger los datos personales en línea, y si son conscientes de sus derechos -privacidad y autodeterminación informativa.

desafíos en cuanto a la facilidad de realizar trámites de servicios públicos en línea durante la pandemia, pues un 48 % de los encuestados reportaron que es difícil o muy difícil y solo un 20 % indicaron que es fácil o muy fácil. En ese mismo estudio se determinó que, 58 % de los usuarios digitales hubieran preferido hacer su trámite presencialmente y que un 29 % manifestó que no volvería a usar Internet para hacer esos trámites. Lo anterior coinciden con lo manifestado por los participantes del presente diagnóstico, ya que estos indicaron que, existe un número limitado de usuarios que confían y realizan trámites de servicios públicos en línea.

214. También se determinó que, el Gobierno de Ecuador no realiza encuestas ni colecta estadísticas sobre el nivel de confianza que tienen los usuarios en los servicios públicos en línea. Sin embargo, de los resultados mostrados por la encuesta del BID se desprende que, los usuarios ecuatorianos prefieren realizar los trámites de forma presencial debido a que son más fáciles, lo cual indica que todavía no todas las personas entienden el uso de la tecnología y de estas plataformas digitales y/o no confían en ese tipo de plataformas digitales para realizar gestiones de servicios públicos.

215. Los participantes también indicaron que las autoridades competentes (e.g., MINTEL, etc.) se toman con seriedad los temas de privacidad, protección de datos personales y seguridad de la información en los portales de gobierno electrónico, por tal motivo, regularmente actualizan sus políticas de privacidad. En esa misma línea, el Plan Nacional de Gobierno Electrónico 2018-2021 (todavía vigente), en su pilar de Gobierno Cercano, se establece que la ciberseguridad es un tema sensible en este ámbito.

216. A inicios de enero del año 2022 circuló en un medio de prensa digital que, en Ecuador, se movieron entre $2.760 millones y $3.220 millones en transacciones de comercio electrónico en el 2021. Según un estudio de la CECE, la frecuencia de las transacciones de comercio electrónico casi que se duplicaron durante la pandemia. Según se determinó, las transacciones de comercio electrónico van en crecimiento, especialmente aquellas en portales nacionales y enfocadas en compra de servicios.

217. Ecuador también ha desarrollado un ambiente propicio para el desarrollo del comercio electrónico, ya que se cuenta con una Estrategia Nacional de Comercio Electrónico (2021) -una iniciativa público-privada- y la Ley de Comercio Electrónico, Firmas y Mensajes de Datos (2002). En dicha estrategia se promueven 4 acciones principales: (i) mejorar el marco legal, lo cual incluye la actualización de la Ley de Comercio Electrónico y su reglamento, (ii) fomentar las actividades de comercio electrónico en las micro, pequeñas y medianas empresas, (iii) mejorar la interoperabilidad del sistema de pago electrónico, y (iv) mejorar la logística en el proceso de comercio electrónico (operadores postales).

218. La CECE maneja una variedad de estadística o métrica con respecto al comercio electrónico en general, pero no se logró obtener información sobre el nivel de confianza que tienen los usuarios en los servicios de comercio electrónico a nivel local. En un reporte de la CECE del 2021 se indicó que antes de la pandemia el crecimiento del comercio electrónico en Ecuador era limitado debido a una serie de factores, entre los cuales figuraba el miedo a las estafas. También se han indicado desafíos tales como la seguridad, manejo y protección de datos personales, entre otros. En todo caso, debido a la pandemia, muchos usuarios se vieron obligados a realizar este tipo de transacciones electrónicas para comprar bienes o servicios que no estaban disponibles de otra forma, lo cual incrementó el número de usuarios de estos servicios.

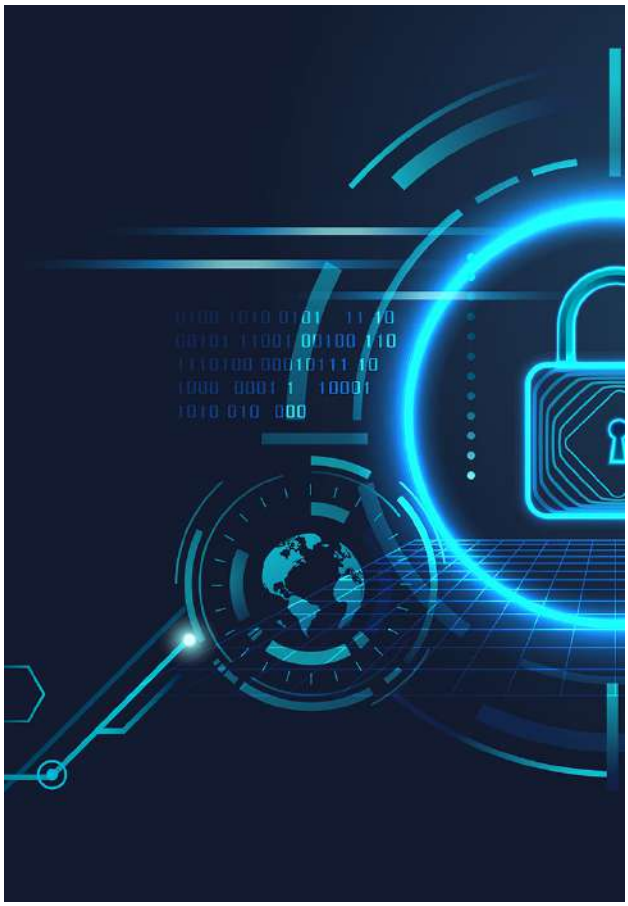
219. También se determinó que el sector privado reconoce la importancia y necesidad de implementar medidas de seguridad para generar confianza en los usuarios de los servicios de comercio electrónico. Como se indicó, el tema de la seguridad y la protección de datos personales son temas sensibles para los usuarios ecuatorianos, así que la mayoría de las plataformas locales usan soluciones confiables de seguridad, así como mecanismos de pago seguro para incentivar el comercio electrónico en el país.

D 2.3 COMPRENSION DEL USUARIO SOBRE LA PROTECCION DE LOS DATOS PERSONALES EN LINEA

Nivel de Madurez: Formativo a Establecido

220. Aunque Ecuador cuenta con la Ley Orgánica de Protección de Datos Personales (LOPDP), la cual entró en vigor desde su publicación -Registro Oficial Suplemento No. 459 del 26 de mayo del 2021- todavía la autoridad de control, a saber, la Superintendencia de Protección de Datos (SPD), no está formalmente establecida. Esta situación generó dudas entre los participantes de sí la implementación de la ley realmente inició a partir de su publicación o iniciará hasta el momento en que la SPD inicie formalmente sus funciones de control.

221. Si bien se han realizado varios Webinars informativos y de concientización, se informó que, todavía no se ha organizado una campaña de concientización a nivel nacional (masiva y potente) sobre el contenido, alcance y aplicación de la LOPDP debido a que todavía la SPD no está establecida.



222. Esta situación hace que tanto los usuarios como otros actores del ecosistema tengan un conocimiento básico de sus derechos y obligaciones, cómo se gestionan los datos personales en entornos digitales y qué buenas prácticas pueden emplearse para proteger sus datos personales en línea. Sin embargo, ese conocimiento básico no es suficiente cuando se tiene una presencia activa en redes sociales y además se usan las TICS de forma intensa. También se mencionó que ese nivel de conciencia va en crecimiento y se espera que mejore con la aplicación de la LOPDP. En esa misma línea, la anterior directora de la Dirección Nacional de Registros Públicos (DINARP) reconoció en una actividad virtual que la SPD deberá "… crear en la ciudadanía esa confianza digital frente a las empresas y el empoderamiento de sus datos personales."

223. También se comentó que a nivel nacional ya se han realizado varios debates y conversatorios académicos sobre la protección de los datos personales en Ecuador, especialmente con motivo de la discusión y aprobación de la LOPDP. Quizá con menor frecuencia, se discute sobre el balance entre la seguridad nacional y la privacidad. En Internet no se logró identificar alguna actividad o conversatorios al respecto, pero los participantes del presente diagnóstico manifestaron que si se ha conversado y debatido sobre el tema.

224. Varios participantes comentaron que tanto instituciones públicas como organizaciones privadas están implementando en sus plataformas digitales y páginas web políticas de privacidad y protección de datos, así como términos y condiciones de uso en cumplimiento con las disposiciones de la LOPDP y el Acuerdo Ministerial No. 12-2019 de MINTEL – el cual aplica únicamente a las instituciones de la administración pública central y que es monitoreado por MINTEL.

D 2.4 MECANISMOS DE DENUNCIA

Nivel de Madurez: Establecido

225. Durante el presente diagnóstico se determinó que, en Ecuador existen varios mecanismos o canales para denunciar delitos informáticos ante las autoridades competentes, a saber, la Policía Nacional, la Fiscalía General, etc. Si lo que se desea reportar es un incidente cibernético, las autoridades ecuatorianas también ofrece otros mecanismos para ese tipo de denuncias (ver D1.2).

226. Los ciudadanos ecuatorianos cuentan con 3 canales para denunciar los delitos informáticos: (1) ante la Fiscalía - Servicios de Atención Ciudadana de la Fiscalía - o

a las unidades de Policía Judicial, (2) al número telefónico de emergencias 911, y (3) a la Policía Nacional mediante el número gratuito 1-800 delito donde se reportan todo tipo de delitos, incluyendo los delitos informáticos. En esa plataforma, los funcionarios trasladan la noticia criminis a la Unidad especializada para iniciar la investigación y contactar a la víctima del crimen.

227. También se determinó que los usuarios de Internet usan las redes sociales e incluso aplicaciones de mensajería instantánea como canales para informar y concientizar a otros usuarios sobre delitos informáticos y otras actividades delictivas.

228. Del año 2019 al año 2021, se presentaron 896 denuncias del delito de apropiación fraudulenta por medios electrónicos, que es el delito de mayor impacto en Ecuador. Seguido del delito de estafa electrónica con 212 denuncias, y el delito de pornografía infantil con 66 denuncias. En los primeros 5 meses del año 2021, ya se habían registrado más 600 denuncias por delitos informáticos, siendo los adultos mayores las principales víctimas de esos delitos. También se informó que tanto la Policía Nacional como la Fiscalía llevan un registro de los delitos denunciados y los casos activos. Es información regularmente se publica en medios de comunicación masiva.

229. El CyberTipline es un sistema centralizado norteamericano para denunciar la explotación infantil en línea. En Ecuador se registraron 242.631 incidentes en el año de la pandemia (2020), un incremento de más del 100 % respecto al 2019. Este mecanismo ha sido de ayuda para descubrir a pedófilos y explotadores sexuales de menores en el país.

Este factor evalúa si la ciberseguridad es un tema de discusión en los principales medios de comunicación y redes sociales. Además, este Factor analiza el papel de los medios de comunicación en la transmisión de información sobre ciberseguridad al público en general, moldeando así sus valores, actitudes y comportamiento en línea sobre ciberseguridad.

D 2.5 MEDIOS DE COMUNICACIÓN Y PLATAFORMAS EN LINEA

Nivel de Madurez: Formativo

230. En Ecuador existe cobertura mediática a los temas de ciberseguridad, pero solo de manera ad hoc. Se realizó un sondeo de los sitios web de noticias más populares del país y se confirma dicha observación, ya que aparecieron muy pocas historias relacionadas con la ciberseguridad y/o delitos informáticos- al menos en los primeros cuatro meses del año 2022. En el año 2021 se observó una mayor cobertura de estos temas.

231. La información y noticias que constan en medios de comunicación, principalmente en plataformas digitales, están relacionadas con incidentes importantes que ocurrieron en Ecuador (e.g., ataques cibernéticos al Banco Pichincha, a Corporación Nacional de Telecomunicaciones (CNT), etc.), a los cuales se le dio una amplia cobertura a nivel nacional. También se observó que, ocasionalmente, se publican reportes, tales como "las 5 tendencias de ciberseguridad para el 2022", "estas serán las peores amenazas en ciberseguridad durante 2022", entre otras noticias de corte informativo. Si se observó que se le da poca cobertura a casos de personas que han sido víctimas de delitos informativos, tales como estafas informáticas, ciberacoso, etc. Se observaron pocos reportajes con ese tipo de información.

232. También se informó que en redes sociales se da cobertura, especialmente cuando ocurren un incidente importante a nivel nacional, y que las personas usualmente comentan y discuten sobre estos temas, pero de forma limitada.

233. También se observó pocos casos de denunciantes de delitos informáticos que hayan tenido un impacto importante a nivel nacional. Si se observaron más casos de denunciantes de situaciones de noticias falsas o que promueven la desinformación con fines políticos y/o para generar caos. Se observó que dos organizaciones ecuatorianas, Ecuador Verifica y Ecuador Chequea, están cumplimiento una función importante en el proceso de identificación de noticias falsas que circulan principalmente en redes sociales y que generaron caos en las dos últimas elecciones presidenciales y durante la pandemia. Esas organizaciones identificaron cientos de publicaciones de esa naturaleza en redes sociales y que, en apariencia, provienen de un expresidente de Ecuador y/o grupos aliados.

234. Así mismo, organizaciones sectoriales, como ASOBANCA, están emitiendo campañas de concientización en los principales medios de comunicación locales, las cuales resaltan que una parte de la seguridad también recae en el buen actuar del usuario.

RECOMENDACIONES

Con base en la información recopilada, se brindan las siguientes recomendaciones que tienen como objetivo proporcionar los pasos a seguir para mejorar las capacidades de ciberseguridad en la presente dimensión siguiendo las consideraciones del modelo CMM.

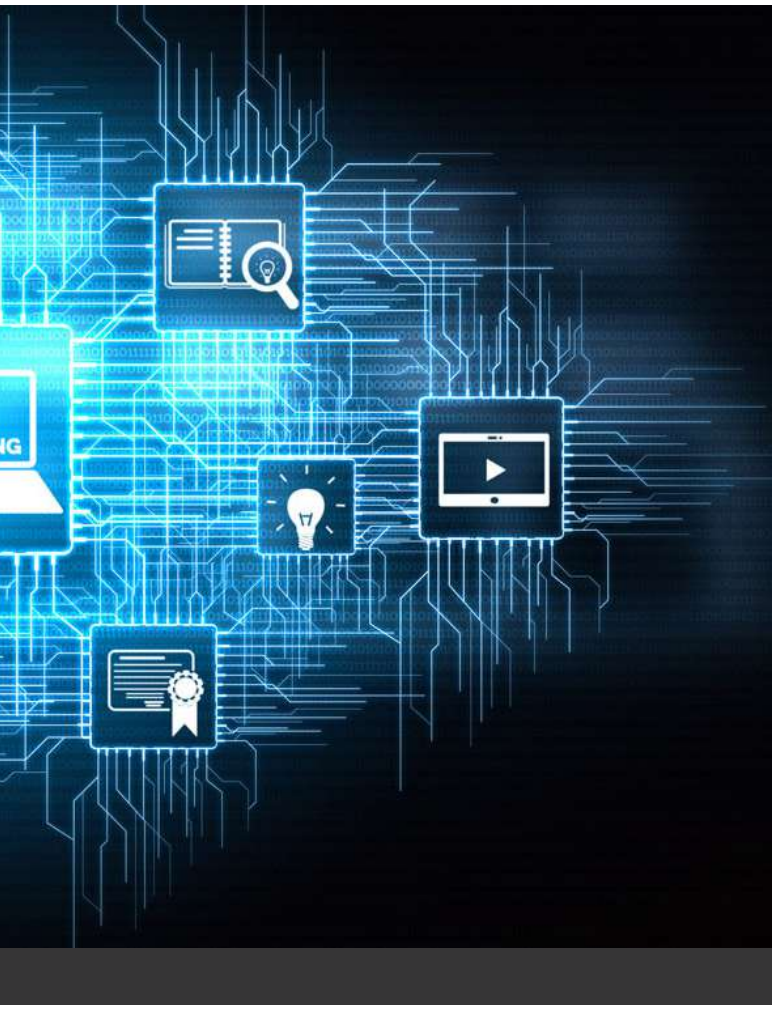
MENTALIDAD EN CIBERSEGURIDAD

R2.1 Asegurarse de que todos los empleados y funcionarios del Gobierno, sin distinción de cargo, reciban periódicamente capacitaciones y/o campañas de concientización sobre temas relacionados con la ciberseguridad de conformidad con un plan y temario previamente definido. Lo anterior con la finalidad de que la ciberseguridad se convierta en un tema prioritario en

todo el sector público y que además los empleados y funcionarios públicos utilicen cotidianamente buenas prácticas de ciberseguridad.

R2.2 Así mismo, considerar la centralización de la administración de esas capacitaciones, y establecer algún tipo de capacitación o inducción sobre ciberseguridad como un componente prioritario en los procesos de incorporación de nuevos empleados.

R2.3 Establecer un programa concientización sobre ciberseguridad, en colaboración con Cámaras de Comercios, Cámaras Industriales u otros actores relevantes del sector privado, dirigido a ejecutivos, empresarios y propietarios de PYMES a efectos de mejorar el nivel de conciencia y entender los posibles riesgos cibernéticos que pueden afectar sus redes e infraestructuras y su impacto en la operación. Lo anterior con la finalidad de que la ciberseguridad se convierta en una prioridad para todos los actores del sector privado y que además todos los actores del sector privado utilicen cotidianamente buenas prácticas de ciberseguridad.



R2.4 Establecer un programa de concientización sobre ciberseguridad, en colaboración con proveedores de Internet u otros actores del sector de telecomunicaciones, dirigido a los usuarios de Internet, con el propósito de mejorar el nivel de conciencia con respecto a los riesgos cibernéticos derivados del uso del Internet. Lo anterior con la finalidad de que la ciberseguridad se convierta un tema prioritario durante sus actividades en Internet y que además los usuarios de Internet utilicen cotidianamente buenas prácticas de ciberseguridad.

R2.5 Incentivar a los proveedores de Internet a crear material de fácil acceso (que se muestren de manera destacada en sus páginas de inicio y se distribuyan a través de sus cuentas de redes sociales) que promuevan tanto buenas prácticas de ciberseguridad como la confianza en sus servicios de Internet.

R2.6 Asegurarse de evaluar periódicamente el nivel de conocimiento que tienen los ciudadanos en Ecuador sobre los temas básicos de ciberseguridad y qué tanto confían ellos en el uso del Internet y los servicios de gobierno electrónico y comercio electrónico lo anterior podría incorporarse en el programa nacional de estadística y censo.

CONFIANZA Y CREEN EN LOS SERVICIOS EN LÍNEA

R2.7 Desarrollar e implementar políticas públicas y/o un marco legal para combatir el impacto de la diseminación de noticias falsas o campañas de desinformación en el país. Mejorar la coordinación multisectorial (fortalecer la relación con Ecuador Verifica y Ecuador Chequea) y la cooperación internacional, establecer medidas regulatorias para las plataformas de servicios de Internet, fortalecer la alfabetización mediática (como una línea de acción en la PNC) y fortalecer las capacidades de monitoreo y evaluación para generar alertas tempranas de forma oportuna (e.g, COCIBER).

R2.8 Desarrollar mecanismos para monitorear del uso de los servicios de gobierno electrónico. Así mismo, difundir campañas en medios de comunicación y redes sociales que destaquen la efectividad y la seguridad de estos servicios. En esa misma línea, se recomienda actualizar regularmente las políticas de privacidad y de notificación a los usuarios de las brechas de seguridad.

R2.9 Asegurarse que el sector privado implementa medidas de seguridad y privacidad para generar confianza en los servicios de comercio electrónico y que además informen a los clientes las soluciones de seguridad implementadas como un mecanismo de mercadeo.

COMPRESIÓN DEL USUARIO SOBRE LA PROTECCIÓN DE LOS DATOS PERSONALES EN LÍNEA

R2.10 Generar conciencia y comprensión entre los usuarios sobre la importancia de la protección de los datos personales en línea y además promover el desarrollo de habilidades para que los usuarios puedan gestionar adecuadamente su privacidad en línea.

R2.11 Promover tanto en la educación primaria y secundaria como en las universidades u otros centros académicos la enseñanza de módulos o contenidos dedicados a la protección de datos personales y privacidad en línea.

R2.12 Establecer alianzas público-privadas con organizaciones de la sociedad civil, el sector privado y el sector académico para integrar el tema de la protección de datos personales en línea en el material de las diferentes campañas de concientización que se están implementando en Ecuador. En este tema, la Superintendencia de Protección de Datos (SPD) -cuando se establezca- deberá asumir un rol importante de coordinación. Ver más detalles sobre la SPD en la Dimensión 4.

R2.13 Fomentar un debate público sobre la protección de los datos personales y sobre el equilibrio entre seguridad y privacidad para informar la formulación de políticas públicas.

MECANISMOS DE DENUNCIA

R2.14 Desarrollar guías y programas de difusión para promover el uso de los mecanismos de denuncia existentes para que el público en general reporte los casos de delitos informáticos, tales como la estafa informática, el ciberacoso, la pornografía infantil en línea, el robo de identidad, entre otros actos delictivos.

R2.15 Así mismo, considerar la posibilidad de establecer una plataforma centralizada e interoperable para que las denuncias de los delitos informáticos sean compartidas en tiempo real a las autoridades competentes (Policía Nacional, Fiscalía, etc.)

R2.16 Informar periódicamente a los niños y adolescentes sobre los mecanismos de denuncia existentes y crear mecanismos de denuncia para esta población.

R2.17 Establecer métricas de efectividad para todos los mecanismos de denuncia existentes en el país y que los resultados informen oportunidades de mejora y la asignación de recursos.

MEDIOS DE COMUNICACIÓN Y PLATAFORMAS EN LÍNEA

R2.18 Establecer un programa para incentivar a los medios de comunicación masiva, incluso aquellos con una presencia activa en redes sociales, a que amplíen la cobertura de los temas de ciberseguridad a aspectos más informativos y se centren en informar al público en general sobre las medidas de ciberseguridad proactivas y viables y el impacto económico y social de los riesgos cibernéticos. Que adopten un enfoque más informativo, sin dejar de lado la difusión de noticias relevantes tanto locales como internacionales.

R2.19 Establecer alianzas entre las autoridades competentes (e.g., MINTEL, EcuCERT, etc.), socios estratégicos (e.g., AECI, etc.) y medios de comunicación para difundir las campañas de concientización existentes en diferentes canales y redes sociales como parte de sus actividades de responsabilidad social corporativa.

R2.20 Fomentar, en todos los niveles y estratos sociales, una discusión crítica y frecuente en redes sociales u otros canales sobre temas relacionados con la ciberseguridad. Así mismo, que las autoridades competentes evalúen esa dinámica en redes sociales u otros medios para informar la formulación de políticas públicas.

DIMENSION 3

DESARROLLO DE CONOCIMIENTO Y CAPACIDADES EN CIBERSEGURIDAD

235. Esta Dimensión evalúa la disponibilidad, la calidad y la aceptación de los programas orientados a varios grupos y sectores, tales como el gobierno, el sector privado y la población en general, y que están vinculados con programas de concientización sobre ciberseguridad, programas de educación formal sobre ciberseguridad y programas de capacitación profesional.

Este Factor se enfoca en la disponibilidad de programas que aumenten el nivel de conciencia sobre temas de ciberseguridad en todo el país, concentrándose en los riesgos y amenazas de ciberseguridad y las diferentes formas de abordarlos.

D 3.1 DESARROLLO DE CONCIENTIZACIÓN EN CIBERSEGURIDAD

Nivel de Madurez: Formativo

236. El Gobierno de Ecuador actualmente no tiene un programa articulado de concientización sobre ciberseguridad a nivel nacional y que esté dirigido a diferentes audiencias, principalmente a grupos vulnerables: niños, adultos mayores, madres solteras, PYMES, etc. Durante las sesiones virtuales se logró determinar que, en Ecuador existen varias campañas de concientización que se implementan de forma independiente (no coordinada) y que son lideradas, principalmente por MINTEL y otras organizaciones de la sociedad civil, academia, y el sector privado.

237. Se comentó que el MINTEL ha generado suficiente contenido para las actividades de concientización sobre ciberseguridad, el cual se encuentra disponible únicamente en su página web. Sin embargo, esas campañas han quedado ahí, no han trascendido y no se han difundido de forma adecuada, manifestaron los participantes.

238. MINTEL también promueve la campaña internacional de concientización denominada “Safer Internet Day”, y que se celebró el pasado ocho de febrero con varias actividades virtuales. Sin embargo, esas actividades no se realizan de forma coordinada y sistemática para lograr un mayor impacto en las comunidades objetivo. Así mismo, participantes del sector público indicaron que MINTEL, en colaboración con Microsoft, Information Systems Audit and Control Association (ISACA), Asociación Ecuatoriana de Ciberseguridad (AECI) y la Policía Nacional, organizó un Webinar denominado “Día del Internet Seguro”, en donde se trató temas como: Consejos prácticos para evitar amenazas en el mundo digital, Internet seguro para niños, ni-

ñas y adolescentes, Una mirada al otro mundo de las pantallas, Ciberdelitos, Civismo, seguridad e interacción en línea; este evento fue retransmitido por la Radio Vigía La voz de la Policía nacional y las redes sociales de todos los organizadores, obteniendo datos como; 12.127 impresiones de publicaciones, 11.889 Alcance de las publicaciones y 613 interacciones con las publicaciones.

239. Se informó que como parte de la implementación del EGSI vo2, MINTEL desarrolló un material para generar conciencia sobre temas de seguridad de la información a los funcionarios del sector público.

240. También se determinó que, en el año 2020 bajo la coordinación del Consejo Nacional para la Igualdad Intergeneracional junto a 22 instituciones públicas, privadas y organismos internacionales se adoptó la política pública por una Internet segura para niñas, niños y adolescentes, cuyo objetivo es proteger la dignidad e integridad física, psicológica, emocional y sexual de la niñez y adolescencia; y potenciar las oportunidades y habilidades que ofrecen las tecnologías digitales en su vida y desarrollo integral.

241. Como parte de la estrategia comunicacional de esa iniciativa, en el año 2020 se creó la página www.internetsegura.gob.ec y que en su oportunidad tenía contenido variado y de alto valor: videos, reportajes, juegos e ideas para niñas, niños, adolescentes, familias y docentes. Sin embargo, esa página actualmente no está activa. En las sesiones virtuales varios participantes comentaron que era una pena que una iniciativa tan importante a nivel nacional haya quedado en nada, al punto de que ni la página web funciona dos años después de la adopción de dicha política pública.

242. Desde el año 2018, AECI está implementando, con recursos propios, la campaña denominada "Seguros en la Red", la cual está dirigida a los niños y adolescentes de la educación primaria y secundaria, y que, mediante personajes lúdicos se cuentan historietas que generan conciencia sobre temas de ciberseguridad. Debido a la pandemia, a inicios del año 2021, la publicación de este material se suspendió, ese material se venía publicando de forma bimensual en una revista local para niños y donde anualmente se llegaron a publicar hasta 45.000 ejemplares. En su momento también se generaron pastillas de concientización con ese mismo material.

243. En el año 2022, la AECI todavía no ha realizado ninguna actividad de difusión, pero se tiene planeado pasar de formato papel a un formato más interactivo, y en esa línea se está trabajando con la Universidad Técnica del Norte para generar más contenido de ese tipo. Algunas instituciones académicas han ayudado en la difusión del material. La AECI intentó establecer algún tipo de alianza con el Gobierno para aprovechar el material existente, pero no se logró un resultado positivo. En una de las sesiones se mencionó que, la AECI nuevamente pone a disposición del Gobierno y la academia el material de dicha campaña para que tenga un mayor alcance e impacto.

244. Desde el año 2015, la Universidad Central del Ecuador (UCE) viene apoyando un proyecto denominado "Internet Segura" – una iniciativa europea- que va dirigido a los niños y adolescentes del país. Para lograr una mayoría difusión, la UCE se ha asociado con otras instituciones.

245. También la Universidad Técnica del Norte (UTN) han realizado campañas sobre el uso de un Internet seguro, donde se difunde material propio y también material producido por la AECI. En esas actividades se han capacitado más de 15 mil niños entre 4 y 15 años y se han establecido convenios con instituciones de educación media -con autorización del Ministerio de Educación- para que de forma extracurricular se brinden capacitaciones y pastillas tanto a los estudiantes como a los docentes y padres de familia.

246. La Escuela Politécnica Nacional desarrolló una iniciativa donde los mismos estudiantes crean contenido de concientización para abordar temas sensibles, tales como cyberbullying, pornografía infantil, etc. para socializarlo a estudiantes del Colegio Don Bosco en la ciudad de Quito. Esa iniciativa se ha implementado en los últimos 4 años, pero de forma intermitente. También se hicieron cursos tipo Massive Online Open Courses (MOOC) sobre ciberseguridad para padres de familia. Además, la UIDE ha realizado actividades de concientización y de fortalecimiento de las herramientas de seguridad de los usuarios finales en colaboración con la empresa Kaspersky.

247. En las sesiones virtuales tampoco se identificó un programa nacional de concientización para ejecutivos. Si se determinó que, existen actividades de concientización aisladas y que son auspiciadas por el gobierno u otros sectores. La AECI colaboró con MINTEL en la realización de una serie de charlas para los CISOs (Chief Information Security Officers) de la administración pública central. En otro momento, la AECI, en colaboración con una Organización No-Gubernamental (ONG) colombiana, realizó unos talleres para los CISOs de instituciones públicas y privadas, pero a la fecha no se ha vuelto a replicar esa iniciativa. Algunas cámaras de comercio y asociaciones gremiales, tales como la AsoBanca, realizan charlas sobre ciberseguridad dirigidas a ejecutivos y altos mandos de las empresas asociadas.

248. Se comentó en una de las sesiones virtuales que, el nivel de conciencia en temas de ciberseguridad de los ejecutivos y directivos todavía es bajo, ya que descono-

cen o tienen un conocimiento limitado en temas básicos de ciberseguridad, tales como la necesidad de mejorar la postura de ciberseguridad de las empresas y el impacto de los riesgos cibernéticos en las organizaciones. Ese nivel de conciencia de los ejecutivos mejora en empresas grandes o transnacionales que brindan servicios esenciales. También se hizo referencia, a un tema de gobernanza, donde los directores y la administración de las empresas delegan totalmente estos temas de ciberseguridad a funcionarios del departamento tecnológico, pero en algunos casos estos tienen un conocimiento limitado o no son experto en ciberseguridad, poniendo en riesgos la infraestructura TIC de las empresas.

249. CEDIA, el CERT coordinador del sector académico, en colaboración con INCIBE España, están impartiendo un curso internacional de formación para CISOs. Así mismo, CEDIA también ofrece cursos técnicos de ciberseguridad y está lanzando un canal en una plataforma digital para difundir noticias y actividades sobre ciberseguridad.

Este Factor evalúa la disponibilidad y provisión de los programas de educación formal en ciberseguridad y además la existencia de catedráticos y profesores calificados para impartir esos programas académicos. Así mismo, este Factor examina la necesidad de mejorar la educación en ciberseguridad a nivel nacional e institucional y la colaboración entre el gobierno, el sector académico y la industria para garantizar que las inversiones en el sector académico satisfagan las necesidades del entorno de educación en ciberseguridad en todos los sectores.

D 3.2 EDUCACION EN CIBERSEGURIDAD

Nivel de Madurez: Formativo a Establecido

250. En la PNC, específicamente en el Pilar 7, se reconoce la obligación que tiene el Gobierno de formular políticas públicas para impulsar la oferta académica en ciberseguridad en el tercer y cuarto nivel, así como promover que las universidades, centros de investigación y otras instituciones académicas incluyan a la educación en ciberseguridad entre sus prioridades de investigación. Sin embargo, los objetivos y líneas de acción de la PNC relacionadas con la educación en ciberseguridad son limitadas y realmente no reflejan las prioridades y necesidades de los diferentes sectores. Este tema fue ampliamente reconocido por los participantes del sector académico.

251. En las sesiones virtuales se comentó que, en Ecuador existen profesionales de altísimo nivel en las diferentes disciplinas de la ciberseguridad (técnica, jurídica, etc.); sin embargo, no todos se inclinan por la docencia o no cuenta con las habilidades pedagógicas necesarias, lo cual genera que el cuadro de profesores especializados y calificados en Ecuador sea limitado y actualmente se encuentre topado.

252. Se determinó que existe una carencia de profesores para cursos especializados, tales como, ingeniería del malware, ciberdefensa, análisis forense, etc. Por tal motivo, varias universidades han optado por contratar a académicos de España u otros países vecinos, con grados académicos de maestría y PhD, para que impartan cursos virtuales. La reubicación de estos académicos en Ecuador es un trámite complejo y costoso, por lo que los cursos virtuales es la mejor opción para satisfacer esa necesidad -y a un bajo costo para no encarecer el costo de las matrículas.

253. También se comentó que la carencia de académicos en ciberseguridad no es un tema relacionado con el salario, ya que las universidades e instituciones académicas respetan los atestados y experiencia de los académicos calificados. También se comentó que no existen programas académicos para la formación de profesores. Tampoco existen políticas públicas para incentivar a profesionales calificados a incursionar en el sector académico.

254. En las sesiones virtuales se comentó que, varias universidades a nivel de pregrado y grado, y en carreras específicas, tales como computación, ingenierías, telecomunicaciones, etc. se imparten cursos que abordan temas relacionados con la seguridad de la información, criptografía, seguridad en redes, seguridad y gestión de riesgos en las IT, etc. Sin embargo, en promedio, solo se imparte un curso relacionado con esos temas en toda la carrera, lo cual resulta insuficiente debido a la importancia que tiene la ciberseguridad en carreras de base tecnológica.

255. Debido a lo anterior, en una sesión virtual se indicó que, las instituciones de educación superior y universidades tienen total autonomía a la hora de incorporar los contenidos, asignaturas o cursos que consideren relevantes, lo cual incluye la posibilidad de integrar más contenidos y asignaturas en el campo de la ciberseguridad y/o la seguridad de la información. Así mismo, la Coordinación de Planificación Académica del Consejo de Educación Superior no revisa o se cerciora si existen cursos o contenidos enfocados en ciberseguridad -todavía no tienen instrucciones en esa línea.

256. En Ecuador existen entre seis o siete programas a nivel de maestría en seguridad informática, ciberseguridad y/o gestión de seguridad de la información -tres programas presenciales y cuatro programas en línea- y que son

impartidos por la UISEK, UDLA, UNIR, UIDE, UTEG, ESPOL, y la PUCE, y algunos casos en colaboración con otras universidades en España. Actualmente, un par de universidades están gestionando la aprobación de maestrías en ciberseguridad, lo cual hace pensar que la demanda va en crecimiento. También se mencionó que la ESPOL tiene un programa de doctorado en ciencias computacionales aplicadas y que tienen contenidos, no cursos, en ciberseguridad.

257. En dos de las maestrías arriba indicadas se abordan temas éticos y legales en su plan de estudio. También se indicó que la UDLA tiene una maestría en Derecho Digital e Innovación, la cual tiene un curso sobre protección de datos personales y otro curso sobre ciberseguridad, seguridad de la información y delitos informáticos. Se indicó que todavía las facultades o escuelas de administración de empresas no integran contenidos o cursos de ciberseguridad dentro de los planes de estudios. Se indicó que es importante darle ese enfoque multidisciplinario a los nuevos profesionales para que tengan una visión más integral del tema.

258. Las universidades que imparten cursos y/o maestría en ciberseguridad o seguridad de la información consideran que existe una demanda importante y que va en crecimiento. La matrícula ronda entre 20 y 30 estudiantes por curso. Así mismo, se informó que las universidades u otros centros de formación superior no llevan métricas ni estadísticas que analicen e informen a la administración sobre la oferta y demanda de los cursos y carreras en ciberseguridad, pero posiblemente algunas universidades llevan algún control de ese tipo, pero de forma limitada.

259. También se indicó que las universidades públicas y privadas no ofrecen becas para los cursos y/o maestrías con énfasis en ciberseguridad. Tampoco existe un programa de becas o fondo de préstamos universitarios enfocados en programas académicos en ciberseguridad. Se indicó que el Instituto de Fomento al Talento Humano tramita las becas para la ciudadanía en general, pero se desconoce si a través de ese instituto se han ofrecido becas o algún tipo de financiamiento a estudiantes en el área de la ciberseguridad o seguridad de la información.

260. En Ecuador no existen iniciativas o políticas públicas que promuevan o incentiven a los estudiantes y profesionales del sector tecnológico a tomar cursos o iniciar una carrera en el ámbito de la ciberseguridad y/o seguridad de la información. En Ecuador las personas que se inclinan por desarrollar una carrera académica y profesional en este sector, es por motivación propia, ya que el gobierno y la industria todavía no ofrecen becas o esquemas de financiamiento, o promueve competencias (e.g., hacktones) u otras actividades para atraer más estudiantes y profesionales a este sector.

261. También se informó en las sesiones virtuales que, en Ecuador todavía no existe una partida específica dentro del presupuesto nacional para promover e incentivar la educación en ciberseguridad, ni mucho menos existe una partida dedicada a la investigación y laboratorios en temas de ciberseguridad, aunque según la PNC el tema de la investigación debería ser una prioridad para las universidades u otros centros de formación superior. Según se indicó, eso todavía no está sucediendo, por falta de recursos.

262. Varias universidades imparten cursos, seminarios y webinars a estudiantes y profesionales no especialistas en ciberseguridad. Otras instituciones y ONGs, como la AECI, constantemente organizan seminarios, webinars, etc. sobre ciberseguridad y otras actividades de formación y concientización para no especialistas.

263. A excepción de los programas de concientización indicados en la D3.1, a nivel de educación primaria y secundaria todavía no se imparten cursos de ciberseguridad ni existen contenidos específicos en los cursos de informática o computación que forman parte de la malla curricular. Se informó que MINTEL ya tuvo un primer acercamiento con el Ministerio de Educación para explorar la posibilidad de incluir temas de ciberseguridad dentro de la malla curricular de la educación primaria y secundaria.

264. Se informó en una de las sesiones virtuales que el gobierno, la academia y la industria todavía no han conformado un grupo de trabajo para revisar regularmente las prioridades y necesidades del sector. Así mismo, se indicó que esa falta de coordinación a nivel nacional entre esos sectores se ve reflejada en la PNC, ya que esa política no cuenta con objetivos estratégicos claros y potentes que aborden las prioridades y necesidades a nivel nacional en el ámbito de la educación de ciberseguridad. Con la revisión a la PNC que MINTEL está liderando, estos temas se deben fortalecer.

Este Factor revisa la disponibilidad y provisión de programas de capacitación profesional en ciberseguridad asequibles para crear un cuadro robusto de profesionales en ciberseguridad en el país. Además, este Factor evalúa la admisión de la formación en ciberseguridad y además la práctica de transferencia de conocimientos y habilidades en ciberseguridad dentro de las organizaciones públicas y privadas, y cómo esta transferencia de habilidades se traduce en una mayor disponibilidad de profesionales en ciberseguridad.

D 3.3 CAPACITACIÓN PROFESIONAL EN CIBERSEGURIDAD

Nivel de Madurez: Formativo a Establecido

265. En la PNC se documentó que en Ecuador se tiene acceso a certificaciones profesionales en ciberseguridad, pero que la mayoría de esas certificaciones son ofrecidas o administradas por entidades internacionales, lo cual genera dependencia tanto para los profesionales como para las instituciones académicas locales. También se indicó que existe un desconocimiento sobre la disponibilidad de dichas certificaciones y algunas son demasiado costosas para el público en general, lo cual es una limitante para que más estudiante y profesionales en seguridad se certifiquen.

266. En Ecuador existe una oferta de programas de capacitación de cursos preparatorios y certificaciones de la industria que abordan temas que van desde las certificaciones en cumplimiento y gestión de IT, certificaciones en seguridad de la IT y otras certificaciones dedicadas a temas de ciberseguridad.

267. En Ecuador varias universidades y centro de formación tienen convenios con varios proveedores de la industria, como el CISCO Networking Academy, en donde se imparten cursos, tanto presenciales como en línea, para obtener certificaciones internacionales en el manejo de equipos y conceptos de conectividad de red e Internet, ciberseguridad, Internet de las cosas, programación y sistemas operativos, entre otros. Otros proveedores como Amazon Web Services, Google, Microsoft también tienen disponibles cursos preparatorios y certificaciones en Ecuador. También en ciberseguridad existen cursos preparatorios y certificaciones de ISACA, IRCA, NEXUS, CISA, COBIT 5 (Control Objectives for Information and Related Technologies), entre otros. Varias universidades han establecido convenios para ofrecer descuentos y facilidades de pago en beneficios de los estudiantes y profesionales en seguridad.

268. Para aquellos profesionales en seguridad que deseen aprender y mejorar sus capacidades en la gestión y respuesta a incidentes, los cursos de Trusted Introducer (Transit I, Transit II, etc.) están disponibles desde Ecuador vía cursos virtuales. Por ejemplo, el equipo de CEDIA es el único equipo en Ecuador con la certificación de Trusted Introducer. No se logró confirmar si el staff del EcuCERT cuenta con esa certificación.

269. En las sesiones virtuales se comentó que en Ecuador existen cursos de capacitación, seminarios u otros recursos en línea, como diplomados en ciberseguridad para profesionales en seguridad. Así mismo, las universidades y centro académicos que imparten esos cursos llevan ciertos controles y estadísticas sobre la admisión y matrícula.

270. En una de las sesiones con el sector académico se presentaron estadísticas de profesionales con certificaciones de ISACA e IRCA, por ejemplo, en CISA existen 46 profesionales certificados, en CISM 21, en CGEIT 2, en CRISC 16, y en CDPSE 16 (corte en diciembre del 2021). Con certificaciones IRCA, en principal auditor 4 profesionales certificados, en Lead Auditor 1, en Auditor 1 y en Associate Auditor 3. Ecuador es un país con una población que ronda los 18 millones de habitantes y aunque el mercado en ciberseguridad es incipiente, es un mercado bastante grande para tener realmente pocas personas con ese tipo de certificaciones.

271. En una de las sesiones virtuales se indicó que la demanda por profesionales con certificaciones de la industria ha crecido en los últimos años, principalmente durante la pandemia, pero la oferta todavía es limitada. Esto último quedó consignado en la propia PNC, cuando se reconoció como un área de mejora; sin embargo, en los objetivos y líneas de acción de la PNC no se establecieron actividades robustas para desarrollar programas de capacitación y promoción de certificaciones de la industria para profesionales en seguridad.

272. Así mismo, varios participantes comentaron que la transferencia de conocimiento en temas relacionados con la ciberseguridad se practica regularmente en Ecuador, principalmente en las empresas del sector privado. En las instituciones públicas no existe una política general en ese sentido; sin embargo, en algunas instituciones se implementa como una buena práctica.

D 3.4 INVESTIGACIÓN E INNOVACIÓN EN CIBERSEGURIDAD

Este Factor evalúa el enfoque que se le da a la investigación e innovación en ciberseguridad para abordar los desafíos tecnológicos, sociales y comerciales y para avanzar en la construcción de conocimientos y capacidades en ciberseguridad en el país.

Nivel de Madurez: Formativo

273.. En el Pilar 7 de la PNC se estableció que, en las universidades, centro de investigación y otras instituciones académicas debían incluirse como una prioridad la investigación en temas de ciberseguridad, pero, nuevamente, no se crearon objetivos o líneas de acción específicas y robustas en esa línea de trabajo.

274. Según se logró determinar en las sesiones virtuales, en Ecuador se están desarrollando pocas actividades en el campo de la investigación y desarrollo con énfasis en ciberseguridad. Se mencionaron varias investigaciones académicas, específicamente tesis de grado y trabajos de investigación que son publicados en revistas especializadas. Existen pocas actividades enfocadas en el campo técnico y/o de innovación, por ejemplo, CEDIA está realizando proyectos de investigación en ciberseguridad y se enfoca en el desarrollo de aplicaciones.

275. Durante el presente diagnóstico no se logró identificar si las universidades u otros centros académicos en Ecuador están interactuando con universidades de la región en el campo de la investigación y desarrollo en temas de ciberseguridad.

RECOMENDACIONES

Con base en la información recopilada en las sesiones virtuales e investigación de escritorio, el equipo de investigación proporciona a Ecuador las siguientes recomendaciones, las cuales tienen como objetivo proporcionar consejos y pasos a seguir para mejorar la capacidad existente en el ámbito de formación y desarrollo de habilidades en ciberseguridad, siguiendo las consideraciones del modelo CMM y buenas prácticas internacionales.

DESARROLLO DE CONCIENTIZACIÓN EN CIBERSEGURIDAD

R3.1 Establecer un programa nacional (coordinado) de concientización sobre ciberseguridad con un plan de implementación detallado. Así mismo, que ese programa este dirigido a concientizar al público en general, especialmente a grupos vulnerables, y que su contenido y material tenga enlaces explícitos a la PNC y su plan de acción.

R3.2 Como parte de dicho programa, generar actividades de concientización para ejecutivos, empresarios y propietarios de PYMES con el fin de concientizar sobre

los riesgos cibernéticos en general, principales métodos de ataques y cómo sus organizaciones pueden gestionar adecuadamente los riesgos u otros problemas cibernéticos.

R3.3 Designar a una entidad coordinadora con el mandato y autoridad suficiente, y los recursos necesarios para llevar a cabo las acciones y actividades de dicho programa.

R3.4 Crear un portal web dedicado para difundir y promocionar el material de dicho programa con el fin de mejorar las habilidades y el conocimiento del público en general, y que, además, ese portal web sea promocionado a través del programa de concientización.

R3.5 Asegurarse que ese programa tenga un plan de seguimiento y revisión que contemple revisiones periódicas de su contenido y material por parte de expertos de diferentes sectores y que además establezcan métricas y estadísticas que permitan evaluar el nivel de efectividad, los avances logrados y la asignación de recursos.

R3.6 Promover una mayor participación del Gobierno y una mejor coordinación a nivel nacional de los programas colaborativos de concientización sobre ciberseguridad liderados por actores del sector privado y de la sociedad civil con el fin de maximizar los recursos y material desarrollados y logran un mayor impacto. Así mismo, definir las funciones y responsabilidades de los actores, los mecanismos de cooperación y las métricas y estadísticas que permitan evaluar el nivel de efectividad, los avances logrados y la asignación de recursos.

EDUCACIÓN EN CIBERSEGURIDAD

R3.7 Crear programas de educación en ciberseguridad para profesores, académicos o instructores con el fin de garantizar la disponibilidad de profesionales calificados, con atestados académicos y experiencia adecuada, que impartan contenidos o cursos de ciberseguridad en el país.

R3.8 Crear incentivos u otros beneficios para que profesionales calificados tanto del sector público como del sector privado se interesen en impartir contenidos o cursos de ciberseguridad en universidades u otros centros de educación superior.

R3.9 Considerar la creación de un grupo permanente de trabajo conformado por representantes de las instituciones públicas encargadas de la coordinación (e.g., Ministerio de Educación, MINTEL, etc.), de la industria y del sector académico para definir e informar las prioridades y necesidades a nivel nacional u otros temas relevantes sobre la educación en ciberseguridad en los procesos de formulación de políticas públicas. Asegurarse que esas prioridades y necesidades nacionales sean consultadas con otros sectores relevantes del ecosistema y que se formen parte de la PNC con líneas de acción robustas.

R3.10 Integrar más contenidos y cursos de ciberseguridad, dándole énfasis a la identificación y mitigación de los riesgos cibernéticos, en todos los programas vocacionales y carreras de base tecnológica que se imparten en los colegios y universidades del país.

R3.11 Promover la creación de más cursos y carreras especializadas de ciberseguridad, delitos informáticos y protección de datos personales en las universidades y otras instituciones de educación superior -que estén acreditadas y en los diferentes grados académicos. También promover la creación de cursos especializados en las diferentes carreras (técnicas -ingenierías- y no técnicas -derecho, administración de empresas, seguridad nacional, criminología, etc.) para suplir las necesidades del mercado.

R3.12 Desarrollar métricas y estadísticas para evaluar periódicamente la oferta y demanda académica de esos cursos, carreras y especializaciones en ciberseguridad para definir e informar las prioridades de educación en ciberseguridad.

R3.13 Promover el carácter multidisciplinario de la ciberseguridad (y sus aspectos técnicos, jurídicos, éticos, comerciales, entre otros) en todos los cursos de la educación superior, así como cursos, seminarios y diplomados sobre temas de ciberseguridad para estudiantes y profesionales sin formación técnica.

R3.14 Promover la inclusión de contenidos o cursos en ciberseguridad, lo cual incluye el uso seguro del Internet y otras plataformas digitales, etc., dentro de la malla curricular de la educación primaria y secundaria. Además, que esos contenidos sean revisados periódicamente.

R3.15 Revisar periódicamente las partidas presupuestarias -dentro del presupuesto nacional- asignadas a la educación en ciberseguridad para asignar recursos suficientes a la atención e implementación de las prioridades y necesidades nacionales en este ámbito de la educación.

R3.16 Asignar recursos financieros adicionales para que las universidades públicas amplíen y mejoren la infraestructura existente -laboratorios, equipos computacionales y otras instalaciones- para satisfacer

adecuadamente demanda de la educación formal en ciberseguridad.

R3.17 Desarrollar programas de pasantías y prácticas profesionales con empresas de la industria para que tanto estudiantes como profesionales adquieran experiencia y desarrollen otras habilidades al combinar la educación y la capacitación práctica.

R3.18 Organizar competencias a nivel provincial y nacional (e.g., hackatones) para poner a prueba las habilidades y destrezas desarrolladas y además se aumente la atracción por las carreras en ciberseguridad.

R3.19 Crear un programa de becas y/o un fondo de préstamos estudiantiles para educación universitaria con el fin de que los estudiantes y profesionales que quieran iniciar o fortalecer el desarrollo de su carrera en ciberseguridad puedan matricularse en programas de académicos y/o certificaciones profesionales.

R3.20 Considerar la posibilidad de crear un plan de incentivos para retener a profesionales calificados no solo en el país sino también en el sector público.

R3.21 Promover y mercadear a la ciberseguridad como una opción de desarrollo profesional con oportunidades de crecimiento profesional y personal.

R3.22 El Gobierno, en colaboración con organizaciones del sector privado y socios internacionales, debería considerar la creación de un centro académico de excelencia en ciberseguridad para la región andina.

CAPACITACIÓN PROFESIONAL EN CIBERSEGURIDAD

R3.23 Evaluar y determinar las necesidades y prioridades a nivel nacional en el ámbito de la capacitación profesional en ciberseguridad para informar la revisión de la PNC y su plan de acción. Esa evaluación podría ser realizada el grupo de trabajo indicado en la recomendación R3.9. Así mismo, desarrollar métricas para evaluar, entre otros temas, los índices de matrícula para fortalecer la oferta académica actual e informar las tendencias y mejoras a los programas de capacitación que existen en el país.

R3.24 Crear un programa de capacitación a nivel nacional para profesionales que cuente con beneficios, incentivos -precios asequibles en certificaciones- e incluso subsidios para desarrollar habilidades específicas, según las demandas del mercado. Así mismo, establecer un grupo de profesionales en ciberseguridad de alto nivel.

R3.25 Como parte de ese programa, se podría considerar la creación de un portal web dedicado a la coordinación y el intercambio de información sobre capacitaciones para expertos, así como crear y mantener actualizado un registro a nivel nacional de exper-

tos y profesionales en ciberseguridad. Así mismo, crear acuerdos con proveedores para ofrecer las diferentes certificaciones de la industria en todas las regiones del país y a precios asequibles.

R3.26 En ese portal web se podría crear una plataforma de networking para organizar eventos relacionados con la ciberseguridad (seminarios, talleres, etc.) y reunir periódicamente a los profesionales en ciberseguridad con fines académicos y sociales. Así como anunciar programas de becas y otras oportunidades académicas que ofrecen organismos o instituciones académicas internacionales.

R3.27 Establecer programas de capacitación o educación continua para profesionales de TI, y profesionales en seguridad en general, en temas de ciberseguridad y/o seguridad informática en todos los sectores.

R3.28 Desarrollar iniciativas que promuevan la creación de más empleos para profesionales y estudiantes en ciberseguridad tanto en el sector público como en el sector privado e incentivar a dichas organizaciones a crear más puestos de trabajo en el área de la ciberseguridad en función de sus necesidades. Así mismo, capacitar periódicamente a su personal de IT para que se conviertan en profesionales en ciberseguridad.

R3.29 Considerar la creación e implementación de políticas internas o incentivos especiales en las instituciones públicas y privadas para retener profesionales calificados en ciberseguridad.

R3.30 Desarrollar e implementar políticas de transferencia de conocimiento en las organizaciones del sector gobierno, organizaciones del sector privado, operadores de IC, entre otros actores.

INVESTIGACIÓN E INNOVACIÓN EN CIBERSEGURIDAD

R3.31 Evaluar y determinar las necesidades y prioridades a nivel nacional en el ámbito de la investigación e innovación en ciberseguridad para informar la revisión de la PNC y su plan de acción. Esa evaluación podría ser realizada el grupo de trabajo indicado en la recomendación R3.9.

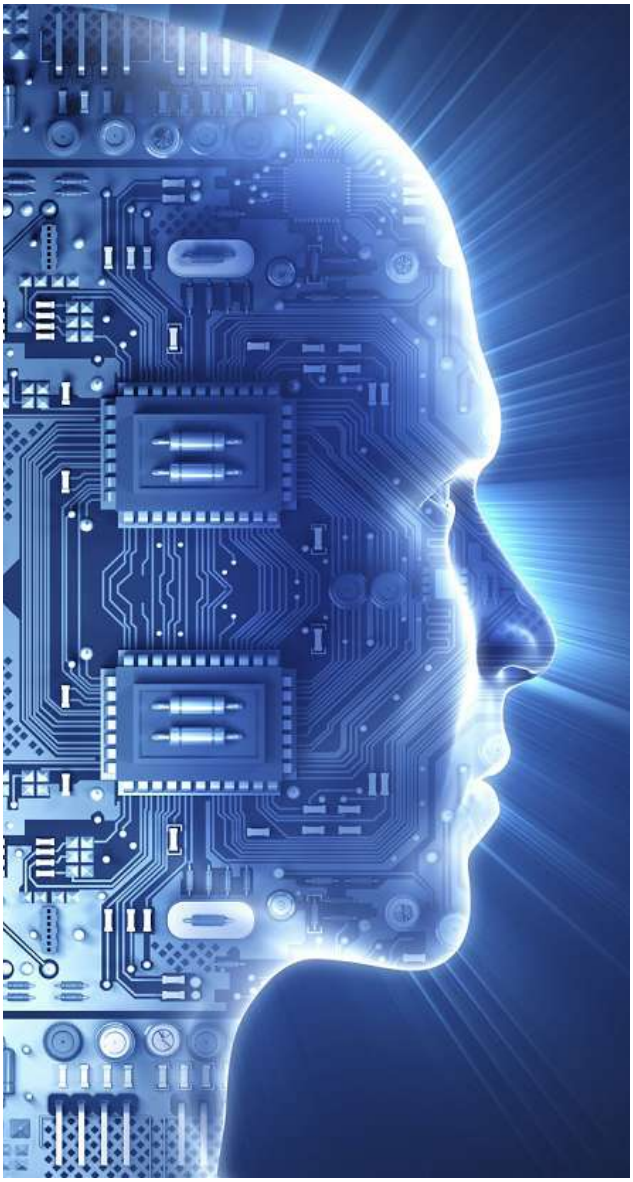
R3.32 Desarrollar métricas para evaluar, entre otros temas, el progreso y mejoras de los diferentes programas de investigación e innovación que existen en el país.

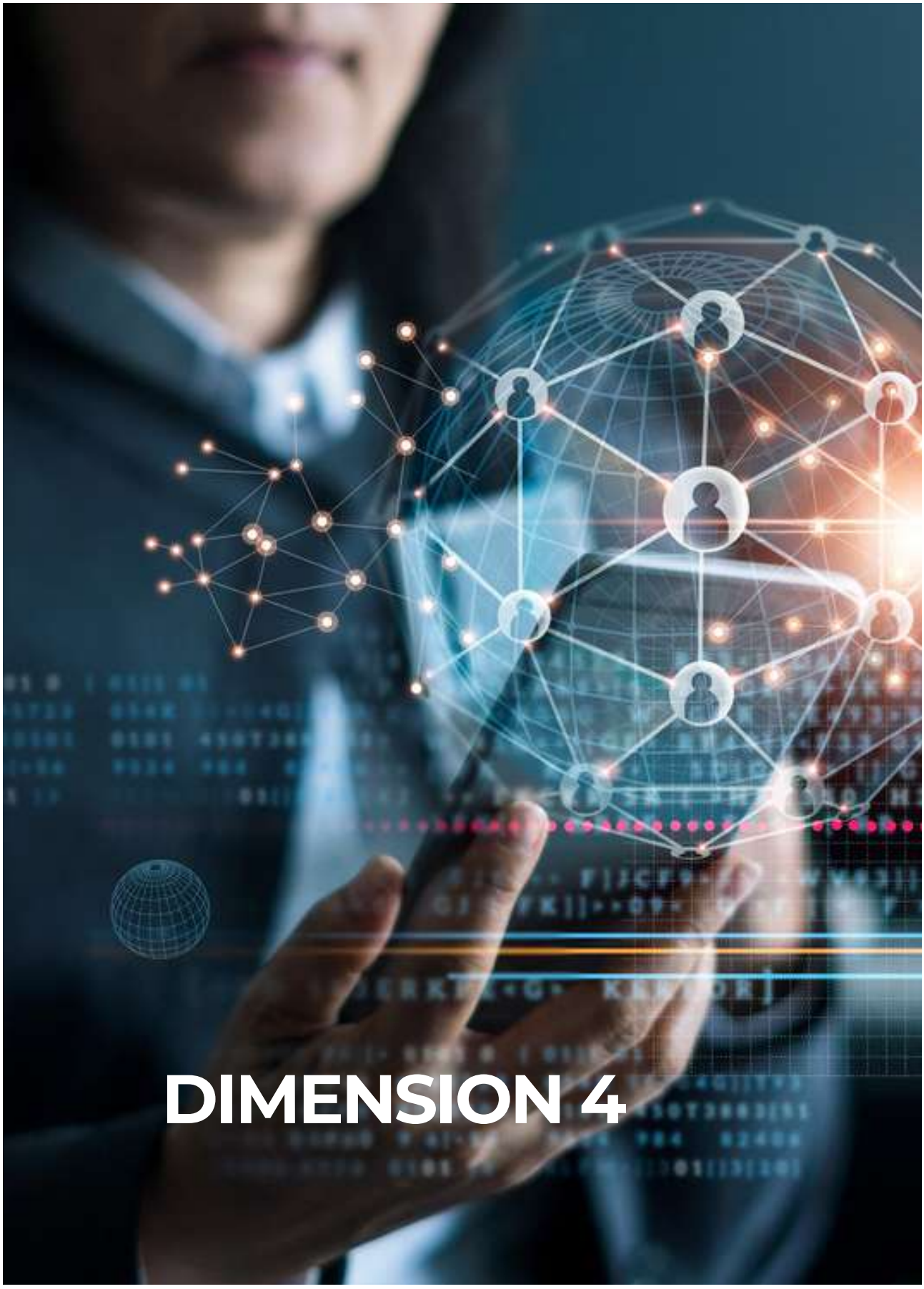
R3.33 Establecer alianzas público-privadas para desarrollar e implementar programas de investigación e innovación (sostenibles y de alto nivel) con universidades y otras instituciones académicas.

R3.34 Asignar recursos suficientes a los programas de investigación e innovación en ciberseguridad en el país.

R3.35 Establecer mecanismos de colaboración con empresas y universidades regionales e internacionales para el desarrollo e implementación de actividades y proyectos de investigación e innovación.

R3.36 Promover la participación de Ecuador en foros y redes de colaboración regionales e internacionales en el ámbito de la investigación e innovación.





DIMENSION 4

MARCOS LEGALES Y REGULATORIOS

276. Esta Dimensión examina la capacidad del Gobierno para formular y promulgar un marco jurídico integral que aborde, directa o indirectamente, aspectos relacionados con la ciberseguridad, con énfasis en requerimientos regulatorios (técnicos y legales), normativa sobre delitos informáticos, entre otros aspectos relacionados. También evalúa la capacidad del Gobierno para hacer cumplir las leyes existentes a través de las agencias de cumplimiento de la ley, la fiscalía, los tribunales de justicia u otros entes reguladores. Además, esta Dimensión observa cuestiones como los marcos de cooperación tanto formales como informales para combatir el cibercrimen en el país.

Este Factor evalúa la existencia de disposiciones legales y regulatorias relacionadas con la ciberseguridad, específicamente sobre requisitos legales y regulatorios en sectores específicos, la legislación sustantiva y procesal sobre delitos informáticos y la evaluación del impacto en los derechos humanos.

D 4.1 DISPOSICIONES LEGALES Y REGULATORIAS

Nivel de Madurez: Formativo a Establecido

277. En varias sesiones virtuales del presente diagnóstico se determinó que, Ecuador aprobó el Código Orgánico Integral Penal (COIP) en el año 2014, y que, en este código penal general, se establece la legislación sobre delitos informáticos, incluidas las disposiciones sustantivas (e.g., tipos penales) y las disposiciones procesales (e.g., prueba documental en formato electrónico).

278. Después de varias reformas, en el COIP se han establecido varios delitos relacionados con el cibercrimen que van desde la pornografía con utilización de niñas, niños o adolescentes (art.103), violación a la intimidad (art. 178), apropiación fraudulenta por medios electrónicos (art. 190), supresión, alteración o suposición de la identidad y estado civil (art. 211), revelación ilegal de bases de datos (art. 229), interceptación ilegal de datos (art. 230), transferencia electrónica de activo patrimonial (art. 231), ataque a la integridad de sistemas informáticos (art. 232), delitos contra la información pública reservada legalmente (art. 233), hasta el delito de acceso no consentido a un sistema informático (art. 234).

279. En la última reforma al COIP del año 2021 se incluyeron o modificaron los siguientes delitos o contravenciones: hostigamiento mediante medios tecnológicos o digitales (art. 154.2), acoso escolar y académico mediante las tecnologías de la información y comunicación (art. 154.3), acoso sexual laboral y ciberacoso (art. 166), abuso sexual y de violación grabado o transmitido mediante medios digitales (art. 170 y 171), extorsión sexual (art. 172.1). Se modificó el texto de los siguientes delitos, revelación de secreto o información personal de terceros (art. 179), interceptación ilegal de datos (art. 230), ataque a la integridad de sistemas informáticos (art. 232), y acceso no consentido a un sistema informático, telemático o de telecomunicaciones (art. 234). También se agregó el delito de falsificación informática (art. 234.1), se establecieron penas agravadas para los delitos de los artículos 232, 234 y 234.1 (art. 234.2), interceptación de las comunicaciones en cooperación internacional (art. 477.1) y se modificó el texto de una contravención relacionada con el descrédito o deshonra de una persona por medios digitales (art. 396) y de la asistencia judicial recíproca (art. 497). Además, en la Ley Orgánica Integral para Prevenir y Erradicar la Violencia contra las Mujeres se estableció la definición de la violencia sexual digital.

280. En materia procesal, en la reforma del año 2021 se hicieron algunos cambios importantes -arriba citados-, pero desde antes ya existían varias disposiciones procesales en el COIP, tales como la interceptación de las comunicaciones o datos informáticos (art. 476), reconocimiento de grabaciones (art. 477), reglas generales sobre la prueba documental (art. 499), y el contenido digital (art. 500). Con las reformas a los artículos 477.1 y 497 en el año 2021 se ha dotado de mejores herramientas a la Fiscalía para investigar los delitos informáticos a nivel nacional -se requieren mejores recursos para la investigación de los delitos transfronterizos. A pesar de lo anterior, todavía se deben mejorar los recursos y la normativa sustantiva y procesal en la lucha contra el cibercrimen, mencionaron algunos participantes de las sesiones virtuales.

281. De las últimas reformas al COIP se desprende que, esos cambios legislativos están orientados a mejorar la legislación de delitos informáticos de Ecuador, así como a alinear al COIP con la normativa del Convenio de Budapest u otros estándares y buenas prácticas internacionales en materia de delitos informáticos.

282. Ecuador todavía no es parte del Convenio de Budapest; sin embargo, el Ministerio de Relaciones Exteriores está trabajando en esa línea y recientemente se envió por medios diplomáticos la solicitud formal de adhesión. En una de las sesiones se indicó que el proceso de adhesión demora 5 años aproximadamente y en ese lapso se debe armonizar la legislación doméstica con las disposiciones del Convenio de Budapest y sus protocolos adicionales. También se comentó que la Fiscalía, con la asistencia técnica de expertos del programa Glacy + del Consejo de Europa, está trabajando en la revisión de la legislación vigente.

283. Así mismo, se informó en una de las sesiones virtuales que, los representantes de Ecuador ante Naciones Unidas están participando activamente en las mesas de trabajo donde se discute el proyecto de la convención internacional exhaustiva contra la utilización de las TIC con fines delictivos.

284. En las sesiones virtuales también se indicó que, en Ecuador todavía no se ha realizado una evaluación de impacto para determinar si la actual legislación de delitos informáticos contemplada en el COIP y otras leyes cumple con los estándares internacionales en protección de derechos humanos. Aunque todavía no se ha realizado esa evaluación de impacto, se comentó que a la fecha no existe ningún proceso de inconstitucionalidad ante la Corte Constitucional donde se esté discutiendo la constitucionalidad de alguna norma del COIP. Tampoco se determinó si durante el proceso legislativo Asambleístas de la República realizaron alguna consulta de constitucionalidad ante la Corte Constitucional y/o se consultaron expertos técnicos y/o juristas expertos en derecho constitucional.

285. Según se informó en varias sesiones que, Ecuador todavía no cuenta con un marco legal y regulatorio que aborde, de forma integral y de aplicación nacional, requerimientos de ciberseguridad, tales como cumplimiento de estándares de seguridad, notificación de incidentes y/o brechas de seguridad, divulgación de vulnerabilidades, entre otros aspectos. Existen ciertas disposiciones legales o normas técnicas que abordan esos temas a nivel sectorial (e.g., EGSI vo2, normas técnicas de los reguladores del sector financiero y de telecomunicaciones) o leyes que abordan temas específicos (e.g., Ley Orgánica de Protección de Datos), pero no como un marco integral y de aplicación nacional. Si se determinó que, los entes regulatorios (MINTEL y su adscrita ARCOTEL, Superintendencia de Bancos, etc.) que han emitido normas técnicas y/o esquemas de seguridad de la información tienen el mandato legal y la capacidad para hacerlas cumplir; sin embargo, se necesitan más recursos y un marco legal y regulatorio más robusto, especialmente en el tema de protección a las infraestructuras críticas digitales y servicios esenciales.

286. Actualmente, existen 5 proyectos de ley sobre ciberseguridad que se encuentran en la Asamblea Nacional. Se desconoce el contenido de esos proyectos de ley, con excepción de dos proyectos, cuyo texto está disponible en fuentes de acceso público. El primer proyecto (2021) se denomina ley orgánica de seguridad cibernética y está enfocado en definir la estructura de gobernanza en ciberseguridad a nivel de gobierno, identificando tanto las instituciones clave como sus funciones y responsabilidades. El segundo proyecto (2019) se denomina ley de seguridad digital y es muy parecido al anterior, pues también se enfoca en el tema de gobernanza. Como se indicó antes, el texto de esos dos proyectos de ley no aborda los temas indicados en el párrafo anterior y además se desconoce si MINTEL o CNC están promoviendo alguno de esos proyectos de ley, o si más bien están trabajando con algún asambleísta en un nuevo proyecto de ley.

****Actualización**

El Gobierno de Ecuador comunicó al Consejo de Europa su interés de adherirse a la Convención de Budapest, mediante la Resolución No. CNC-2021-002 del 28 de octubre del 2021 del Comité Nacional de Ciberseguridad.

A solicitud de MINTEL y basado en información suministrada por dicho ministerio, se actualiza la Dimensión 4, específicamente el factor D.4.1 "Disposiciones Legales y Regulatorias", sustentada en los siguientes avances:

La Cancillería del Ecuador está liderando el proceso de adhesión al Convenio de Budapest, de acuerdo con sus competencias y cumpliendo la Resolución del Comité Nacional de Ciberseguridad. El Ecuador remitió al Consejo de Europa, a través de la Embajada del Ecuador en Bélgica, la Nota oficial expresando el INTERÉS DEL PAÍS DE ADHERIR A LA CONVENCIÓN SOBRE CIBERDELINCUENCIA, conocida como "CONVENCIÓN DE BUDAPEST".

La Secretaría del Comité del Convenio procesó la solicitud ecuatoriana y la sometió a consulta a los Estados miembros. En vista de que no hubo objeciones, el 1 de abril de 2022, la Dirección de la División de Derecho Internacional Público y Oficina del Tratado, informó al Ecuador que el Comité de Ministros del Consejo de Europa durante su sesión número 1430, de 30 de marzo de 2022, decidió extender una invitación a Ecuador para que acceda a la Convención. Particular que fue informado a la presidenta del Comité Nacional de Ciberseguridad mediante Oficio N.º MREMH-SAM-2022-0256-O, el 2 de abril de 2022.

El Ecuador tendrá la calidad de observador en el Comité del Convenio y dispondrá de cinco años para finalizar el proceso de ratificación del instrumento. En esta etapa, el país deberá adoptar las medidas necesarias para que su legislación esté en concordancia con el Convenio de Budapest y sus protocolos adicionales.

Del 10 al 13 de mayo de 2022, se realizó en Estrasburgo, la vigésimo sexta Reunión Plenaria del Comité de la Convención de Budapest, en la cual Ecuador participó, por primera vez, en calidad de Estado observador. En el marco de dicha reunión, la presidenta del Comité de la Convención de Budapest saludó la presencia de Ecuador y recordó que la invitación del Consejo de Europa tiene una vigencia de cinco años, hasta el 30 de marzo de 2027. La delegación ecuatoriana aprovechó la oportunidad para presentar el interés del Ecuador en continuar recibiendo cooperación en el proceso de adecuación legislativa, a través de los proyectos Glacy+, Octopus y otros mecanismos de cooperación disponibles.

4.2 MARCOS LEGISLATIVOS RELACIONADOS

Este Factor evalúa la existencia de disposiciones legales y regulatorias relacionadas con la ciberseguridad, específicamente sobre requisitos legales y regulatorios en sectores específicos, la legislación sustantiva y procesal sobre delitos informáticos y la evaluación del impacto en los derechos humanos.

Nivel de Madurez: Establecido

287. La Constitución Política de la República de Ecuador en su artículo 66, inciso 19 establece que, a las personas se le reconocerá y garantizará el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

288. En el año 2021, Ecuador adoptó la Ley Orgánica de Protección de Datos Personales (LOPDP) -publicada en el Registro Oficial Suplemento No. 459 del 26 de mayo del 2021-, la cual entró en vigor desde su publicación y se dio un plazo de dos años de adecuación para entrar a funcionar el sistema sancionatorio. Se comentó que la LOPDP fue desarrollada con la cooperación internacional del Consejo de Europa y del Banco Interamericano de Desarrollo. Sin embargo, a la fecha, dicha ley no cuenta con una autoridad de control debido a que no se ha establecido formalmente la Superintendencia de Protección de Datos (SPD) -autoridad rectora y encargada de velar por el cumplimiento y supervisión de las disposiciones tanto de la LOPDP como de su reglamento -todavía sin aprobar.

289. Según se indicó, el nombramiento del Superintendente de Protección de Datos estará a cargo del Consejo de Participación Ciudadana y Control Social (CPCCS), basado en la terna propuesta por el Presidente de la República de conformidad con el artículo 77 de la LOPDP. El CPCCS ya aprobó el reglamento para la selección del Superintendente.

290. Actualmente, la Secretaría de Asuntos Jurídicos de la Presidencia está revisando tanto el borrador del reglamento de la LOPDP -redactado por la DINARP- como el borrador del reglamento de selección del Superintendente. Así mismo, el Presidente también está revisando la partida presupuestaria de la operación de la SPD. Todavía no se tiene una fecha exacta de cuándo la SPD iniciará funciones.

291. Como la entidad de control, SPD, todavía no está establecida, se cuestiona si la LOPDP se hará cumplir hasta que se establezca la SPD. También se mencionó que la DINARP no está realizando actividades de control, ya que su función es de coadyuvante en el proceso de control y protección de datos personales en Ecuador.

292. Se comentó que, en la medida de lo posible, la LOPDP está alineada con los estándares y buenas prácticas internacionales en la materia. También se indicó que no es una ley perfecta, tiene falencias importantes y en algunos temas es confusa, pero se puede mejorar en los próximos años. Muchos de los temas confusos se trataron de enmendar vía reglamentaria. En el primer borrador de la LOPDP se incluyó el derecho al olvido, pero luego fue borrado y no forma parte del texto actual de la ley.

293. La LOPDP requiere que tanto instituciones públicas como privadas nombren un delegado de protección de datos, y en el reglamento (todavía sin aprobar) se establecerán los requisitos mínimos para ser nombrado como tal, no incluye la obtención de una certificación. También se indicó que la DINARP el año pasado emitió una serie de normas técnicas en materia de protección de datos para el sector público.

294. En caso de una brecha de seguridad, la LOPDP establece que el responsable del tratamiento deberá notificar a la SPD y a ARCOTEL dentro de los 5 días naturales desde su descubrimiento, y la notificación al titular de los datos se realizará dentro de los 3 días naturales desde su descubrimiento.

295. Como se indicó en la D3.1, en el año 2021, Ecuador adoptó la política pública por una Internet segura para niños, niñas y adolescentes, y en su Eje 1, medidas legales, se establecieron acciones relacionadas con el fortalecimiento de la normativa para promover los derechos digitales y la dignidad e integridad física, psicológica, emocional y sexual de niños, niñas y adolescentes, estableciendo mecanismos para el aprovechamiento de los beneficios de las TICs y mecanismos de mitigación de los riesgos y delitos que pueden cometerse a través de ellas. Lo anterior incluía reformas al Código de Niñez y Adolescencia, al COIP, entre otras actividades. En una de las sesiones virtuales se indicó que, dicha política pública no quedó en nada; se desconoce realmente si esa política está en marcha y está teniendo el impacto esperado, o si actualmente está en pausa y/o bajo revisión, producto del cambio de gobierno.

296. En esa misma línea, como se indicó en la D4.1, al COIP se le realizaron varias reformas en el 2021, en las cuales se mejoró la legislación de delitos informáticos relacionada con la niñez y la adolescencia, incorporándose los delitos indicados en la D4.1. Así mismo, el Código de Niñez y Adolescencia no ha corrido con la misma suerte, actualmente se discute en la Asamblea Nacional una reforma integral que dará origen al Código Orgánico de Protección Integral de Niñas, Niños y Adolescentes, el cual se espera que, tal y como se definió en dicha política pública, se haga la inclusión y reconocimiento de los derechos digitales y las capacidades y medidas de protección y reparación frente a las transgresiones y delitos cometidos contra la niñez y adolescencia.

297. También se indicó que tanto esa política, como las reformas al COIP y el proyecto de ley del Código Orgánico de Protección Integral de Niñas, Niños y Adolescentes, están basadas en estándares y buenas prácticas internacionales en la materia. En Ecuador el nivel de conciencia sobre la protección de la niñez y adolescencia en línea es medianamente alto, y también se avanza a nivel de políticas públicas y de legislación. Incluso a nivel de la Corte Constitucional se han conocido casos de violencia contra la niñez y adolescencia -se mencionó un caso reciente de sexting a nivel colegial.

298. La legislación sobre la defensa al consumidor en Ecuador tiene sustento constitucional en los artículos 52, 53, 54, 55 y 66 de la Constitución Política, y la protección del consumidor en línea a nivel general está regulada en la Ley Orgánica de Defensa del Consumidor (2000) y en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002) y su reglamento. Según se comentó en las sesiones virtuales, esos cuerpos legales deben actualizarse porque tienen casi 20 años de existencia, y con el impulso que ha tenido el comercio electrónico producto de la pandemia, la realidad de Ecuador en este campo ha cambiado sustancialmente, así que esos instrumentos legales deben adecuarse a las nuevas circunstancias.

299. La Ley de la Defensa del Consumidor es transversal para todo tipo de relación comercial y se encarga de regular las relaciones entre proveedores y consumidores, promoviendo el conocimiento y protegiendo los derechos de los consumidores y procurando la equidad y la seguridad jurídica en dichas relaciones entre las partes. Por otro lado, la Ley de Comercio Electrónico garantiza los derechos del consumidor con relación al uso de los servicios electrónicos; al derecho a la libertad de elección o para aceptar los mensajes de datos; y, al derecho a la información acerca del objeto de adquisición o relación electrónica. La última reforma del reglamento a la Ley es con el Decreto Ejecutivo No. 867, publicado en Registro Oficial 532 de 12 de septiembre del año 2011. El reglamento de esta Ley ha sido actualizado mediante el Decreto 13/56 del año 2008. La última reforma a la Ley fue publicada mediante Registro Oficial Suplemento 180 de 10 de febrero del año 2014. Cuando se aprobó la Ley de Comercio Electrónico publicada mediante Registro Oficial 557 del 17 de abril del año 2002, se realizaron reformas al COIP, dando origen a infracciones informáticas en Ecuador como son: acceso no autorizado, falsificación informática, fraude informático, daños informáticos, y violaciones al derecho a la intimidad.

300. Se informó que existe normativa y normas técnicas a nivel sectorial, en donde se reconoce ampliamente los derechos de los usuarios, por ejemplo, en el sector financiero (bastante desarrollado) y en el sector de telecomunicaciones. También se indicó que la Defensoría del Pueblo, a través de la Defensoría Adjunta del Consumidor y Usuario, es la entidad rectora de la defensa del consumidor en Ecuador.

301. También se determinó que, Ecuador cuenta con una Estrategia Nacional de Comercio Electrónico (ENCE) que pretende fomentar la generación de capacidades en los diversos actores de la economía, para una mayor y eficiente participación en las transacciones en línea, la adopción tecnológica, y a su vez, establecer marcos institucionales y normativos uniformes que podrán apoyar significativamente al desarrollo comercial y la interoperabilidad transfronteriza, considerando que la economía mundial es una economía digital. La ENCE está a cargo de MINTEL y del Ministerio de Producción, Comercio Exterior, Inversión y Pesca, y tal y como se indicó anteriormente, la ENCE propone realizar un diagnóstico de las leyes arriba indicadas u otros instrumentos legales. Se desconoce qué tanto se ha avanzado en la implementación de la ENCE y en la actualización de esas leyes.

302. El tema de protección de la propiedad intelectual en Ecuador está a cargo del Servicio Nacional de Derechos Intelectuales (SENADI). Además, Ecuador forma parte de la Organización Mundial de Propiedad Intelectual (OMPI/WIPO) desde 1988.

303. En materia normativa de Protección Intelectual, Ecuador aprobó en el año 2021 el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, en donde se regula, en otros temas, el software y bases de datos, tecnologías libres y formatos abiertos, nombres de dominio, entre otros aspectos. Así mismo, Ecuador ha ratificado varios convenios internacionales en el tema en cuestión, pero especialmente los convenios denominados WIPO Copyright Treaty y el WIPO Performances and Phonograms Treaty, también conocidos como los convenios de Internet por la propia OMPI/WIPO, ya que establecen normas internacionales destinadas a prevenir el acceso no autorizado y el uso de obras creativas en Internet u otras redes digitales. Ecuador ratificó ambos convenios desde el año 2002.

Este Factor evalúa la capacidad de las fuerzas de aplicación de la ley para investigar los delitos informáticos, la capacidad de la fiscalía para investigar y presentar casos de delitos informáticos y las pruebas electrónicas, y la capacidad de los tribunales de justicia para presidir y juzgar los casos de delitos informáticos y aquellos que involucran pruebas electrónicas y/o que son casos de delitos transfronterizos. Finalmente, este Factor revisa la existencia de organismos reguladores intersectoriales para supervisar el cumplimiento de la normativa específica de ciberseguridad.

D 4.3 CAPACIDAD Y COMPENTENCIA LEGAL Y REGULATORIA

Nivel de Madurez: Formativo a Establecido

304. En el año 2011, la Policía Nacional creó la Unidad de Delitos Tecnológicos, que tiempo después pasó a llamarse la Unidad de Delitos Cibernéticos (Unidad especializada). Esta Unidad especializada tiene su centro de operaciones en la ciudad de Quito, pero su jurisdicción sobre delitos cibernéticos es a nivel nacional.

305. Esta Unidad especializada está conformada por 21 investigadores y agentes policiales para todo el país, con experiencia tanto en la parte investigativa como en la parte técnica. Estos agentes inician el proceso investigativo una vez que el incidente es denunciado a la Fiscalía, la cual verifica la tipicidad penal de la conducta denunciada y luego delega la investigación en dicha unidad investigativa.

306. En el año 2021, se procesaron en promedio 1.851 investigaciones (algunas todavía en curso), lo cual implica que cada agente tiene a su cargo un promedio de 200 investigaciones, así que la carga laboral es muy alta y eso impide avanzar más rápido en las investigaciones. Del año 2019 al año 2021, esta Unidad especializada realizó la investigación y proporcionó la evidencia necesaria para que 46 personas fueran privadas de su libertad por la comisión de delitos informáticos. Así mismo, ya se condenó a la primera persona, a 33 años de cárcel, por la comisión del delito de pornografía infantil.

307. La mayor parte del tiempo laboral de los investigadores y agentes de esta Unidad especializada se dedica a cumplir los requerimientos de la Fiscalía, lo cual implica la realización de entrevistas a las víctimas, reconocimiento del lugar del incidente, recopilación de la evidencia digital, etc. y toda esa información tiene que ser consignada en un informe para la Fiscalía, el cual tiene un plazo de entrega. El resto del tiempo, en realidad limitado, lo dedican a la parte investigativa.

308. En una de las sesiones virtuales se comentó que, debido al desconocimiento de algunos fiscales y otras autoridades, los cuales asumen que, por el hecho de usarse medios tecnológicos en la comisión de un delito, estos deben ser investigados por esta Unidad especializada, lo cual genera una saturación de trabajo y se cuenta con recursos limitados. Debido a lo anterior, las autoridades están gestionando duplicar el recurso humano de esta Unidad especializada y habilitar otro centro de operaciones, posiblemente en la ciudad de Guayaquil, para poder descentralizar y dar un mejor servicio a nivel nacional. Uno de los desafíos de esta Unidad especializada es la disponibilidad de recurso humano con las competencias idóneas.

309. Esta Unidad especializada depende financieramente de la Policía Nacional y se cuenta con recursos limitados para la operación. Actualmente, esta Unidad especializada necesita mejorar los recursos y herramientas tecnológicas, tanto hardware como software. Esta Unidad especializada no tiene un laboratorio forense científico, pero las investigaciones forenses se trabajan con la Unidad de Criminalística y su departamento de informática forense, las cuales tienen peritos acreditados que se encargan de los procedimientos para garantizar la cadena de custodia (levantamiento y fijación de la prueba, etc.) y la integridad de la evidencia.

310. Esta Unidad especializada sigue las políticas de capacitación interna de la Policía Nacional, en donde se requiere de la realización de cursos especializados, pero no es claro si esta Unidad especializada tiene un plan de capacitación interno. En el año 2021, 40 investigadores y agentes policiales realizaron el primer curso de especialización en ciberdelitos. Para el año 2022, la Policía Nacional tiene un plan bastante ambicioso de capacitación y para ello ya se trabaja con el Instituto Universitario de Policía Nacional para que ofrezca una carrera especializada en delitos informáticos a nivel universitario, lo cual ayudaría a mejorar las capacidades de la Policía Nacional en temas de cibercrimen.

311. Esta Unidad especializada también está trabajando en la creación de la Universidad de la Policía Nacional, un proyecto que va en curso y que recientemente fue aprobado por la Asamblea Nacional. Actualmente, un total de 20 investigadores y agentes policiales están cursando la maestría en delitos informáticos en la UNIR (modo virtual), los cuales pasarán en su momento a fortalecer la operación de esta Unidad especializada.

312. En el año 2022, esta Unidad especializada tiene planeado implementar un programa de ciberpatrullaje, usando herramientas Open-Source intelligence (Osint) o Web Intelligence (Webint), para monitorear las actividades en Internet que tienen un impacto directo en el país, y así generar las alertas tempranas de forma oportuna y proceder con las investigaciones.

313. Aunque no es su función principal, la Unidad especializada a través de la Policía Nacional, participa activamente en la difusión de campañas de concientización, por medios de comunicación masivos y charlas, y que son dirigidas al público en general, escuelas, etc.

314. Por otro lado, la Fiscalía General de la República

todavía no tiene una unidad especializada de delitos informáticos y, en términos generales, sus recursos también son limitados. Sin embargo, ya se analiza la posibilidad de crear una unidad especializada en delitos informáticos para mejorar el servicio.

315. En una de las sesiones virtuales se mencionó un curso de especialización de delitos informáticos, que tuvo una duración de 7 meses, y donde asistieron 5 funcionarios de Fiscalía, entre ellos, 3 fiscales y 2 servidores administrativos. Justamente, esos 3 fiscales son los encargados de desarrollar la unidad especializada dentro de la Fiscalía, y al parecer son los únicos fiscales que cuentan con formación especializada en temas de delitos informáticos y evidencia digital.

316. La Escuela de Fiscales de Ecuador ha realizado varias capacitaciones sobre delitos informáticos. También se indicó que Estados Unidos también ha dado capacitaciones a los fiscales. La Unidad especializada de la Policía Nacional y la Fiscalía han desarrollado canales de comunicación y colaboración muy efectivos. Constantemente la Policía Nacional invita a los fiscales a que participen en cursos cortos, capacitaciones y seminarios sobre delitos informáticos. De hecho, a la capacitación sobre Sistema Ciberfísico dotado por la Embajada de Gran Bretaña, para la lucha de delitos informáticos (CPS) participaron 10 fiscales -ver abajo más detalles.

317. Se comentó que las autoridades competentes están fortaleciendo los mecanismos de colaboración entre la Fiscalía y el Centro de Inteligencia del Ecuador, ya que este centro cuenta con varios recursos e insumos de inteligencia (alerta temprana) que pueden ser de utilidad para la Fiscalía y otras instituciones públicas.

318. En varias sesiones virtuales se indicó que, la mayoría de los jueces desconocen a profundidad los delitos informáticos y los temas técnicos, como el reconocimiento de la evidencia digital. Sin embargo, en el país si existen algunos jueces con conocimiento básico y/o avanzado sobre delitos informáticos y evidencia digital -incluso algunos han escrito libros sobre el tema-, pero quizá por un tema de competencia y/o jurisdicción -por falta de coordinación administrativa- estos jueces especializados no están conociendo y resolviendo los casos de delitos informáticos.

319. También se comentó que, de los 3 actores del sector de justicia criminal, la función judicial tiene capacidades más limitadas en el ámbito de los ciberdelitos. El Consejo de la Judicatura desde hace tiempo no realiza capacitaciones sobre evidencia digital u otros temas relevantes para resolver casos de delitos informáticos. Los jueces, en general, no comprenden los temas técnicos relacionados con los delitos informáticos.

320. La Escuela de la Función Judicial constantemente ofrece capacitaciones sobre varios temas, y ocasionalmente aborda el tema de delitos informáticos y evidencia digital. Con este tipo de capacitaciones se pretende formar la mayor cantidad de jueces para desarrollar un cuadro de jueces con los conocimientos adecuados para la judicialización de los delitos informáticos en el país. La Escuela de la Función Judicial también capacita a defensores públicos y fiscales.

321. En su momento, el Consejo de la Judicatura le envió a la Corte Suprema de Justicia una encuesta sobre el levantamiento de necesidades, o sea sobre temas prioritarios y donde se requiere capacitación, y entre ellos fi-

guraba los delitos informáticos, así que, a nivel de la Judicatura, están conscientes de la necesidad de invertir más en capacitación para formar jueces con las capacidades y competencias idóneas para conocer y resolver este tipo de casos.

322. Así mismo se determinó que, algunos reguladores sectoriales en Ecuador están conscientes de que deben extender sus actividades de control a temas de ciberseguridad y para ello deben emitir normas técnicas y regulaciones en este campo a efectos de mejorar y garantizar la disponibilidad de los servicios esenciales que ofrecen las entidades reguladas. En el país, tanto MINTEL, a través de ARCOTEL, como la Superintendencia de Bancos han avanzado en este aspecto y ya han adoptado varias normas técnicas sobre temas específicos. Sin embargo, se ocupan mejores recursos técnicos para monitorear y supervisar su cumplimiento, emitir normas técnicas más integrales y asignar suficientes recursos.

323. También se indicó que es urgente que reguladores de otros sectores en donde la ciberseguridad todavía no es un tema regulado o prioritario (e.g., distribución de agua potable, salud, energía, etc.), mejoren su postura regulatoria e integren los temas prioritarios de ciberseguridad en el esquema regulatorio.

324. Como se indicó en la D1.3, todavía no se han identificado las infraestructuras críticas nacionales ni mucho menos se ha establecido un marco regulatorio general en temas ciberseguridad para los servicios críticos y/o esenciales, así que las autoridades competentes (MDN, MINTEL, etc.) todavía no tienen claridad en cuanto al modelo de gobernanza que se implementará en ese ámbito, lo cual incluye la posibilidad de establecer un regulador intersectorial o que más bien esa función de control recaiga sobre los reguladores sectoriales existentes. De igual forma, estos deben actuar de forma proactiva en aras de garantizar la entrega oportuna del servicio y empezar a regular de forma integral los aspectos sensibles en el ámbito de la ciberseguridad de conformidad con los estándares y buenas prácticas internacionales.

325. En el sector público, específicamente en la administración pública central, MINTEL ya inició el proceso de auditoría del EGSI Versión 2.0, específicamente en las instituciones que ya tiene un nivel de implementación del cien por ciento. Las instituciones que no han logrado ese nivel de implementación van poco a poco integrando ese esquema en las actividades diarias de su operación. La falta de recursos económicos y tecnológicos y de personal capacitado hacen que ese proceso sea más lento en algunas instituciones.

326. El MINTEL regularmente emite lineamientos preventivos de ciberseguridad a las entidades públicas que están dentro de su campo de acción, y además realiza visitas de evaluación de cumplimiento (in situ) a más de 90 instituciones.

327. En el ámbito de la protección de datos personales, todavía no se ha establecido formalmente la Superintendencia de Protección de Datos, pero las autoridades competentes (Presidencia y Consejo de Participación Ciudadana y Control Social) ya están trabajando en el proceso de nombramiento y de asignación de recursos (ver D4.2).

****Actualización**

Se creó la "Unidad Nacional Especializada en Investigación de Ciberdelito" en la Fiscalía General de Estado, mediante la Resolución 34 FGE-2022 del 8 de junio del 2022.

A solicitud de MINTEL y basado en información suministrada por dicho ministerio, se actualiza la Dimensión 4, específicamente el factor D.4.3 "Capacidad y Competencia Legal y Regulatoria", sustentada en los siguientes avances:

Mediante Resolución 34 FGE-2022 del 8 de junio de 2022, la Fiscalía General del Estado, creó la "Unidad Nacional Especializada en Investigación de Ciberdelito", que tiene a su cargo la investigación de los delitos tipificados en el Código Orgánico Integral como son: revelación ilegal de base de datos, interceptación ilegal de datos, transferencia electrónica de activo patrimonial, ataque a la integridad de sistemas informáticos, delitos contra la información pública reservada legalmente y acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

Esta Unidad tendrá su sede única en la ciudad de Quito y un ámbito de investigación a nivel nacional, pudiéndose extender a otras provincias conforme a la necesidad institucional. Dicha resolución establece las atribuciones y conformación de la Unidad. Es responsabilidad de la Fiscalía General del Estado, establecer el plan de implementación correspondiente para dar cumplimiento a la Resolución 34 FGR-2022.

Este Factor aborda la existencia y funcionamiento de mecanismos de cooperación formales e informales que permiten la interacción y colaboración entre actores nacionales y transfronterizos para disuadir y combatir el cibercrimen en el país.

D 4.4 MARCOS DE COOPERACION FORMAL E INFORMAL PARA COMBATIR EL CIBERCRIMEN

Nivel de Madurez: Formativo a Establecido

328. La Unidad especializada tiene una buena relación y comunicación tanto con Ministerio de Defensa como con el COCIBER, con quienes tiene una relación más directa y fluida. Incluso, en el año 2021, la Unidad especializada fue invitada y participó en un simulacro sobre juego de guerra que organizó el COCIBER. También tienen una buena relación y comunicación con MINTEL, ARCOTEL y el EcuCERT. Incluso forman parte de la Red Nacional de Confianza administrada por el EcuCERT.

329. Esta Unidad forma parte del Comité Nacional de Ciberseguridad y en el seno del Comité se han propuesto la adhesión de Ecuador al Convenio de Budapest, y para ello, la Cancillería, MINTEL, Fiscalía, Ministerio de Gobierno y otras organizaciones están promoviendo esa iniciativa a efectos de que Ecuador forme parte de la Red 24/7 y además tenga acceso a una serie de recursos que facilitan la lucha contra el cibercrimen.

330. Durante las sesiones virtuales se informó que la Unidad especializada tiene una buena relación con algunos actores del sector privado, especialmente con los operadores de telefonía móvil u otros sectores relevantes, con quienes han desarrollado canales de comunicación y colaboración bastante sólidos. Se indicó que antes el trámite para la obtención de información de usuarios era muy engorrosa y normalmente se entregaba a destiempo (demoraba 2 o 3 meses). Recientemente, se mejoraron los procedimientos a través de sistemas informáticos para que la Policía Nacional pueda solicitar, por medio de una unidad especializada, esa información de forma directa, más expedida y en formato digital (ahora demora 24 horas). La Policía Nacional está buscando implementar un sistema similar, pero con los más 300 de proveedores de servicios de internet en el país, (ISPs por sus siglas en inglés), donde actualmente los procedimientos son también engorrosos y poco eficientes y que afectan la investigación.

331. Se determinó en las sesiones virtuales que, no existe una coordinación interinstitucional ni se ha trazado una hoja de ruta de cooperación entre la Policía Nacional, la Fiscalía General y la Judicatura para mejorar los procesos, comunicación, recursos y conocimiento a efectos ser más eficientes en la investigación y judicialización de los delitos informáticos en el país. Sin embargo, la cooperación que se brinda actualmente se enfoca en la parte investigativa y en la parte de capacitaciones. Es importante que estos tres actores formen un grupo de trabajo para definir una hoja de ruta con la finalidad de fortalecer sus capacidades y trabajar de forma coordinada.

332. Con respecto a la investigación de delitos transfronterizos, esta Unidad especializada tiene una buena relación con sus pares de Colombia y Perú por medio de POAC.

333. La relación con proveedores de servicios de Internet fuera del territorio ecuatoriano es compleja y no siempre se obtienen los resultados deseados. Esta Unidad especializada gestiona los requerimientos de información a través de los portales que los proveedores de servicios de Internet (e.g., Facebook, WhatsApp, etc.) tienen disponibles, pero ellos deciden que casos son importantes

y prioritarios – en los cuales se da una respuesta relativamente rápida-, mientras que en otros casos -que ellos catalogan de poco relevantes- ni siquiera responden. Se indicó que es importante que se generen mecanismos o políticas públicas que obliguen a los operadores de servicios de Internet que brindan el servicio en Ecuador a dar una respuesta más expedita.

334. La Unidad especializada tiene buena relación con las agencias de cumplimiento de ley internacionales (e.g., INTERPOL, EUROPOL, AMERIPOL, etc.), pero cuando se recurre a mecanismos de asistencia legal mutua para judicializar los requerimientos de información, los plazos son mucho más extenso y poco eficientes -pueden demorar hasta un año la obtención de información. En esa línea, se hace urgente que Ecuador se adhiera Convenio de Budapest para formar parte de la Red 24/7 y cualquier otro mecanismo que facilite el intercambio de información.

335. Esta Unidad especializada también trabajan con socios estratégicos, tales como PAcCTO (un programa, financiado por la Unión Europa, de asistencia contra el crimen organizado transnacional), la Embajada de Estados Unidos, la Embajada de Gran Bretaña, entre otros. Actualmente, esta Unidad especializada está trabajando con la Embajada de Estados Unidos, quien le ha dotado de un sistema denominado NIMIC, sistema informático que generan alertas tempranas de información de pornografía infantil que pueden tener su origen en Ecuador, lo cual les permite iniciar la investigación de forma expedita. También colaboran con la Embajada de Gran Bretaña, quienes les han dotado de un sistema denominado CPS, similar el NIMIC. A inicios del 2022, se capacitaron 10 servidores policiales en CPS.

336. A través de PAcCTO, que es el nexo directo con EUROPOL, dicha Unidad especializada forma parte de la Red Cibel@, una plataforma destinada a la lucha contra el cibercrimen en Europa y América Latina, y que permite intercambiar información y organizar capacitaciones, asistencias técnicas para mejorar la capacidad investigativa en el país. En el año 2021, Ecuador fue la sede de la Reunión Anual del PAcCTO, y donde participaron los directores de las unidades de cibercrimen de los países miembros. Se espera que en el año 2022 los miembros del PAcCTO generen una campaña regional de concientización sobre las criptodivisas.

RECOMENDACIONES

Después de analizar la evidencia presentada y recopilada durante los grupos focales con respecto a los marcos legales y regulatorios de ciberseguridad, se realizan las siguientes recomendaciones a Ecuador. Estas recomendaciones tienen como objetivo proporcionar consejos y pasos a seguir para mejorar la capacidad de ciberseguridad existente, siguiendo las consideraciones del modelo del CMM.

DISPOSICIONES LEGALES Y REGULATORIAS

R4.1 Evaluar periódicamente, con la colaboración y asistencia de socios internacionales (e.g., Consejo de Europa), las disposiciones sustantivas y procesales del COIP en materia de delitos informáticos y cualquier otro marco regulatorio en el ámbito de la ciberseguridad para identificar vacíos y brechas normativas, y cualquier otro cambio o actualización de conformidad con las necesidades y entorno nacional e internacionales.

R4.2 Establecer mecanismos para armonizar continuamente el marco legal y regulatorio de ciberseguridad de conformidad con los objetivos de políticas públicas -incluyendo la PNC, tratados regionales e internacionales (e.g., Convenio de Budapest) y buenas prácticas.

R4.3 Asegurarse que las leyes y reglamentos sobre temas de ciberseguridad sea ampliamente discutidas y consultadas con los actores relevantes del ecosistema.

R4.4 Promover y acelerar el proceso de adhesión al Convenio de Budapest, principalmente, y también considerar la adhesión al Convenio Lanzarote y al Convenio 108 Plus, todos administrados por el Consejo de Europa.

R4.5 Fortalecer el marco legal y regulatorio existente mediante la incorporación de leyes y reglamentos que aborden temas como la protección de las infraestructuras críticas digitales y servicios esenciales, u otros requerimientos técnicos como la obligatoriedad del uso de estándares de seguridad en organizaciones públicas y privadas, notificación de incidentes cibernéticos o brechas de seguridad, divulgación responsable de vulnerabilidades, intercambio de información, etc.

R4.6 Como parte de la evaluación indicada en la recomendación R4.1, (i) evaluar el nivel de efectividad en la aplicación y cumplimiento de esas leyes, así como la capacidad, autoridad y recursos de las instituciones públicas rectoras para monitorear y hacer cumplir esas leyes, y (ii) evaluar si las disposiciones sustantivas y procesales del COIP y cualquier otra disposición legal relacionada con delitos informáticos, u otros marcos regulatorios sobre ciberseguridad cumplen con los estándares y buenas prácticas internacionales de protección de derechos humanos u otros derechos fundamentales.

R4.7 Asegurarse que tanto la legislación nacional como el sistema judicial reconocen y protegen los derechos humanos en entornos digitales, y que el público en general entiende y conoce los recursos y vías legales disponibles para valer sus derechos fundamentales en entornos digitales. Así mismo, promover la investigación y el debate nacional sobre los derechos humanos en Internet.

MARCOS LEGISLATIVOS RELACIONADOS

R4.8 Como parte de la evaluación indicada en la recomendación R4.1, evaluar las leyes y reglamentos relacionados con la protección de los datos personales, protección de la niñez y adolescencia en línea, protección al consumidor en línea, comercio electrónico, y propiedad intelectual de bienes y servicios digitales para que dichas leyes cumplen con estándares y buenas prácticas internacionales y se ajusten a las necesidades y al entorno nacional e internacionales.

R4.9 Establecer la Superintendencia de Protección de Datos (SDP) dentro de un plazo razonable y que dicha autoridad de control cuente con suficientes recursos

financieros y tecnológicos, capital humano capacitado y la autoridad suficiente para cumplir con su mandato.

R4.10 Asegurarse que la SDP tiene, dentro de su agenda de actividades, la organización de una campaña de concientización a nivel nacional (masiva y potente) sobre el alcance y aplicación de la LOPDP y su reglamento.

R4.11 Evaluar el proceso de implementación de la política pública por una Internet segura para niñas, niños y adolescentes y, de ser necesario, asignar más recursos y realizar los ajustes necesarios para mejorar o retomar el proceso de implementación.

CAPACIDAD Y COMPETENCIA LEGALES Y REGULATORIA

R4.12 Asegurarse que la Unidad de Delitos informáticos de la Policía Nacional tenga los recursos y capacidades de investigación avanzadas que permita la investigación de casos de delitos cibernéticos complejos y transfronterizos.

R4.13 Asegurarse que esta Unidad cuenta con suficientes recursos financieros y tecnológicos y capital humano capacitado para cumplir con su mandato legal.

R4.14 Asegurarse que esta Unidad y otras agencias de la Policía Nacional tengan establecidos y documentados los protocolos y procedimientos para velar por la integridad de la prueba y la cadena de custodia de la prueba, y además se cumplan los estándares internacionales de recolección de evidencia en las investigaciones nacionales y transfronterizas.

R4.15 Evaluar las necesidades inmediatas de esta Unidad y en esa línea asignar más recursos para la contratación de investigadores o agentes calificados. Así mismo, definir un plan anual de capacitación que incluya temas más sofisticados y especializados en función de sus prioridades y necesidades.

R4.16 Crear una fiscalía especializada de delitos y contravenciones informáticas, y a su vez dotarla de suficientes recursos financieros y tecnológicos y de capital humano calificado. Definir un plan anual de capacitación que incluya temas más sofisticados y especializados en función de sus prioridades y necesidades.

R4.17 Considerar la posibilidad de que esa fiscalía especializada tenga oficinas, con recursos suficientes, en las principales regiones del país o en las zonas con mayor incidencia de delitos informáticos.

R4.18 Identificar los jueces que tienen interés y conocimiento avanzado en temas de delitos informáticos para formar un grupo de jueces especialista en la materia y que sean ellos los que conozcan y resuelvan los casos de delitos informáticos en el país.

R4.19 Considerar la posibilidad de que la Escuela de la Fiscalía y la Escuela de la Función Judicial desarrollen de forma conjunta tanto un programa coordinado de capacitaciones periódicas como un programa académico (robusto) a nivel de maestría para especializar investigadores de la Policía Nacional, fiscales y jueces en materia de delitos informáticos y evidencia digital.

R4.20 Asegurarse que los entes reguladores de sectores específicos o servicios esenciales (e.g., telecomunicaciones, financiero, energía, transporte, etc.) incorporen a los marcos regulatorios normas técnicas robustas en material de ciberseguridad y que además tengan la autoridad, los recursos tecnológicos y financieros, y el capital humano calificado para monitorear y supervisar el cumplimiento de las normas técnicas.

MARCOS DE COOPERACIÓN FORMAL E INFORMAL PARA COMBATIR EL CIBERCRIMEN

R4.21 Establecer mecanismos formales de comunicaciones y un marco normativo que promueva y obligue el intercambio periódico de información entre organizaciones de los sectores público y privado con el fin de combatir el cibercrimen en el país.

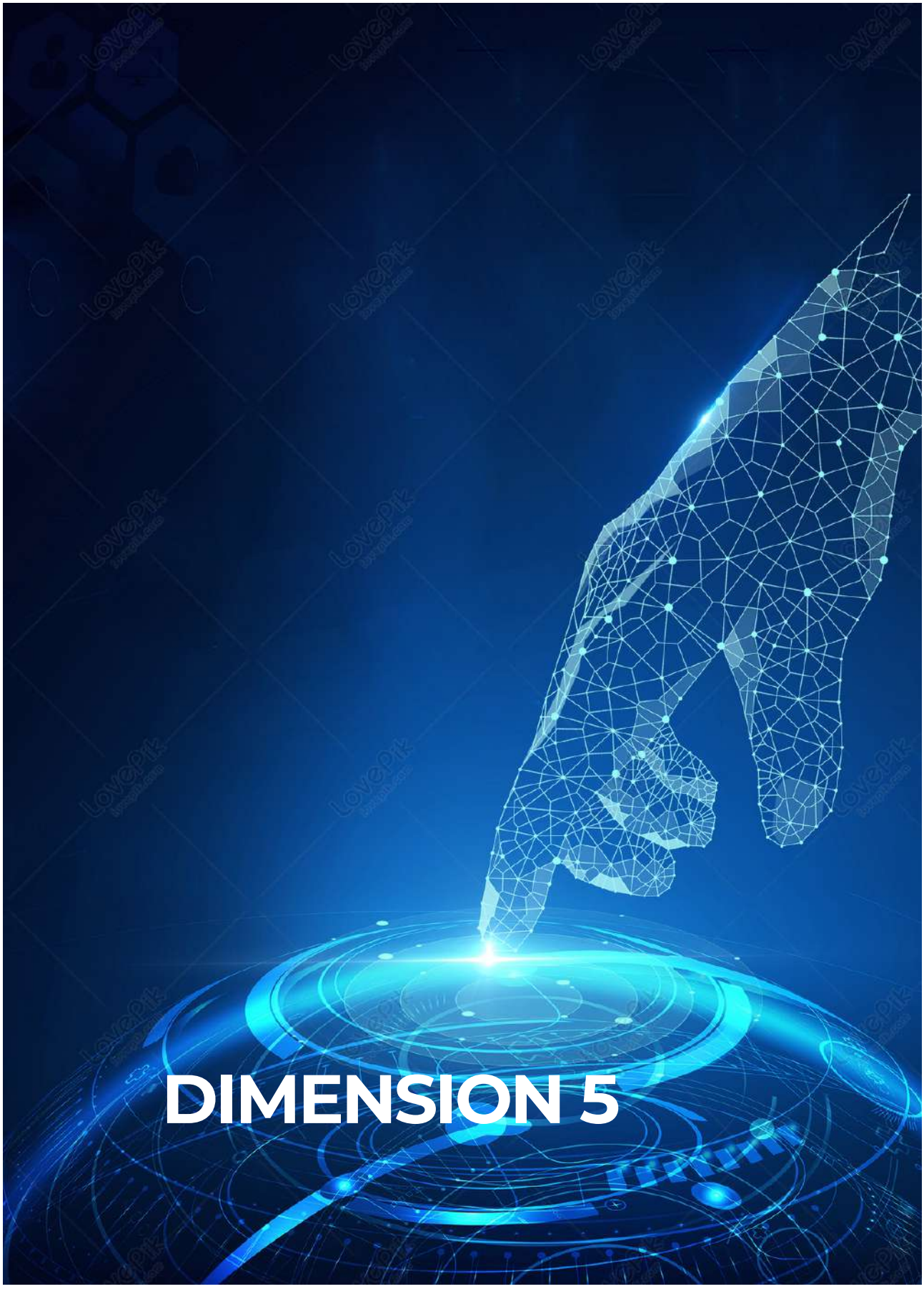
R4.22 Fortalecer los mecanismos formales de cooperación entre los proveedores de servicios de Internet nacionales y la Policía Nacional, específicamente la Unidad especializada, con canales de comunicación claros y efectivos para combatir el cibercrimen en el país.

R4.23 Mejorar los mecanismos de comunicación con los proveedores de servicios de Internet y otras tecnologías ubicadas fuera del territorio ecuatoriano, e incluso establecer acuerdos de cooperación con puntos focales para mejorar los tiempos de respuesta en los requerimientos de información para las investigaciones.

R4.24 Fortalecer los mecanismos formales de cooperación internacional entre la Policía Nacional, específicamente la Unidad especializada, y las agencias de cumplimiento de la ley internacionales (e.g., INTERPOL, EUROPOL, AMERIPOL, etc.) para facilitar la detección, investigación y acusación del cibercrimen. Así mismo, asegurarse que la Policía Nacional, específicamente la Unidad especializada, forma parte de las redes de colaboración internacionales.

R4.25 Evaluar la efectividad de los mecanismos de cooperación internacional existentes, tales como convenios de asistencia legal mutua y tratados de extradición, para mejorar su funcionamiento e incluso establecer acuerdos con otros países, según los índices de incidencias de delitos transfronterizos.

R4.26 Fortalecer los mecanismos formales de comunicación e intercambio de información y buenas prácticas entre investigadores de la Unidad especializada, fiscales y jueces con la finalidad de garantizar investigaciones y procesos judiciales eficientes y expeditos - justicia pronta, oportuna y sin dilaciones- en los procesos de delitos informáticos.



DIMENSION 5

ESTANDARES Y TECNOLOGIAS

337. Esta Dimensión evalúa el uso efectivo y generalizado de las tecnologías de ciberseguridad para proteger a las personas, las organizaciones y la infraestructura nacional. Así mismo, esta Dimensión examina específicamente la implementación de estándares y buenas prácticas de ciberseguridad, el despliegue de procesos y controles, y el desarrollo de tecnologías y productos para reducir los riesgos cibernéticos y mejorar la resiliencia cibernética de las organizaciones públicas y privadas.

Este Factor revisa la capacidad del Gobierno para promover, evaluar la implementación y monitorear el cumplimiento de estándares y buenas prácticas internacionales de ciberseguridad.

D 5.1 CUMPLIMIENTO DE ESTANDARES

Nivel de Madurez: Formativo a Establecido

338. Se determinó que, en la PNC, en el segundo pilar y en sus líneas de acción se menciona seguir estándares de seguridad de la información, pero si se requiere fortalecer e incentivar la implantación de estándares de seguridad tanto en las instituciones públicas como en las organizaciones del sector privado.

339. En Ecuador el cumplimiento e implementación de estándares de seguridad en el ámbito de las TIC es variado, depende mucho de la naturaleza y tamaño de la organización y el sector en donde opera. Debido a que se están mejorando los niveles de concienciación a nivel corporativo, cada vez más, instituciones públicas y privadas deciden adoptar una postura más responsable, y por ende, comienzan a invertir más recursos en ciberseguridad e implementan este tipo de estándares de seguridad, principalmente como una buena práctica, o incluso porque el mismo mercado demanda ese tipo de actividades para garantizar la disponibilidad del servicio- ya algunos usuarios un poco más sofisticados lo ven como un elemento diferenciador entre los proveedores, pues está en juego la privacidad y seguridad de sus datos personales.

340. En el sector público, específicamente en la administración pública central, las instituciones están obligadas a cumplir con el EGSI Versión 2.0, elaborado con base en la norma ecuatoriana NTE INEN-ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 y que es un compendio basado en las normas de la familia de la ISO 27.000. La implementación del EGSI Versión 2.0 es supervisada por MINTEL. Actualmente, MINTEL está evaluando a las instituciones públicas que reportaron un nivel de cumplimiento del cien por ciento.

341. En el portal , MINTEL ha desarrollado varios reportes de seguimiento y guías, tales como la guía de implementación del EGSI Versión 2.0, la guía para la gestión de riesgos de seguridad de la información, la guía para la implementación de controles de seguridad de la información, entre otros documentos. Según se informó que, no todas las instituciones sujetas al cumplimiento del EGSI vo2 han logrado un nivel de implementación del cien por ciento; sin embargo, MINTEL está realizando una labor de supervisión y acompañamiento para asegurarse que el nivel de implementación sea total dentro del plazo estipulado por MINTEL, el cual ya fue ampliado. En ese portal, existe un ranking de cumplimiento del EGSI que está vigente al mes de setiembre del año 2020. Este ranking muestra que la gran mayoría de las instituciones obligadas anda entre el 70 % y el 90 % de implementación.

342. MINTEL definió que el 31 de enero de cada año, las instituciones obligadas a la implementación del EGSI Versión 2.0 deberán remitir el Informe de Cumplimiento de la Gestión de Riesgos. En dicho portal, como se indicó, existen reportes de cumplimiento, y en las estadísticas del año 2020, se observaban instituciones públicas que ofrecen servicios críticos, tales como salud pública, finanzas, registro de datos públicos, etc. que todavía no habían cumplido con los entregables estipulados en el esquema de cumplimiento propuesto por MINTEL -pero posiblemente si están implementando el EGSI vo2.

343. Las empresas privadas, catalogadas como grandes y/o transnacionales, principalmente en el sector fi-

nanciero y telecomunicaciones, tienen un nivel de madurez más avanzado en este ámbito y han desarrollado su propio esquema de seguridad de la información basado en estándares y buenas prácticas internacionales, tales como ISO 27.001 (entre otras de la familia ISO 27.000), ISO 22.301, NIST, entre otras.

344. Como se indicó en la D1.3, algunos reguladores, como ARCOTEL y la Superintendencia de Bancos, han emitido normas técnicas de ciberseguridad para abordar temas específicos, pero no con un enfoque integral. Así mismo, en el caso de empresas transnacionales, la misma casa matriz u oficina regional requieren que se cumplan no solo estándares de seguridad generales (e.g., ISO 27.001) sino también estándares de seguridad de la industria (e.g., NERC) para garantizar la disponibilidad y continuidad del servicio. Dichos reguladores supervisan y auditan que algunos de esos estándares de seguridad son implementados.

345. También se determinó que una cantidad importante de empresas privadas, quizá en el rango de empresas pequeñas y medianas (e.g., PYMES), e incluso unas pocas instituciones públicas, todavía no implementan estándares y buenas prácticas de seguridad.

346. En Ecuador, el tema de la implementación de estándares de seguridad en los procesos de compras/adquisición de bienes o servicios es muy similar a lo descrito anteriormente. En términos generales, tanto las instituciones públicas como las organizaciones privadas implementan los lineamientos establecidos por el estándar ISO 27.001 en el ámbito de la relación con proveedores en los procesos de compras de servicios y productos.

347. Así mismo, en el EGSI Versión 2.0 específicamente en el control 11, se establecen una serie de medidas y recomendaciones aplicables a las relaciones con proveedores, tales como las políticas de seguridad de la información en relación con proveedores, requisitos de seguridad en contratos con terceros, cadena de suministro de tecnologías de la información y la comunicación, gestión de la provisión de servicios del proveedor y monitoreo y revisión de los servicios de proveedores, etc. Algunas instituciones públicas, además de cumplir con el EGSI Versión 2.0, también aplican como buena práctica la implementación de estándares como el COBIT 2019, ITIL v4 u otros esquemas de seguridad para asegurar la calidad de los productos y servicios.

348. En Ecuador la implementación de estándares de seguridad relacionados con la provisión de bienes y servicios es similar o inferior a la implementación de los estándares de seguridad arriba indicados.

349. En el sector público, MINTEL es el ente rector en el ámbito de la implementación de las tecnologías de la información y comunicación. Mediante el Plan Nacional de Gobierno Electrónico se adoptó el Código Orgánico de Economía Social de los Conocimientos, Creatividad e Innovación (Código Ingenios), el cual promueve que las instituciones públicas usen software de fuente abierta y sea desarrollado en el país, como primera opción. Posteriormente, se adoptó el Reglamento para la adquisición de software por parte de las entidades contratantes del Sector Público (Decreto Ejecutivo N. 1073), para reglamentar correctamente el art. 148 del Código Ingenios, el cual incentiva la innovación y desarrollo de la industria del software en Ecuador.

350. El artículo 7 de dicho reglamento crea el Portal Único de Software Ecuatoriano (https://www.softwarepublico.gob.ec/), el cual es gestionado por MINTEL y opera como un catálogo único de la oferta de software de cualquier modalidad con valor agregado ecuatoriano. Este catálogo integra la información contenida en el catálogo de software publicado en el Sistema de Información de Ciencia, Tecnología, Innovación y Saberes Ancestrales y el catálogo de la oferta nacional de software.

351. Con respecto a los procesos de compras públicas, los procesos estandarizados en el ámbito contractual los administra el Servicio Nacional de Contratación Pública (SERCOP), el cual regula las garantías de calidad del hardware, provisión de servicios administrados y servicios cloud por parte de organizaciones del sector público y privado.

352. En el sector privado, las organizaciones con políticas de seguridad robustas, ya sea que están en la industria del desarrollo de software, o contratan el desarrollo de un software a la medida, o contratan un servicio hospedado en la nube, se aseguran de que el software o la aplicación en la nube hayan cumplido con prácticas seguras durante el ciclo de desarrollo del software (e.g., estándares y pruebas de seguridad Open Web Application Security Project (OWASP)).

D 5.2 CONTROLES DE SEGURIDAD

Este Factor evalúa la evidencia sobre el despliegue de controles de seguridad por parte de los usuarios y las organizaciones del sector público y privado. Así mismo, evalúa si el conjunto de controles tecnológicos de ciberseguridad se basa en marcos de ciberseguridad establecidos.

Nivel de Madurez: Formativo a Establecido

353. En el presente diagnóstico se determinó que, en Ecuador se están implementando una variedad de controles técnicos de seguridad tanto por parte de los usuarios finales como por parte de las instituciones públicas – a través de la implementación de EGSI vo2- y las organizaciones privadas -basadas en el estándar ISO 27.002-, posiblemente no de forma consistente en todos los sectores.

354. Según se informa, tanto instituciones públicas como organizaciones privadas implementan controles técnicos, tales como antivirus e implementan parches de software -que para muchas instituciones se actualizan automáticamente, procedimientos de administración de contraseñas, así como controles de seguridad física para centros de datos (data centers), y respaldos o copias de seguridad (backups) que se realizan de forma periódica y se almacenan tanto en instalaciones internas como externas.

355. Así mismo, tanto organizaciones grandes del sector privado como instituciones públicas que ofrecen servicios en plataformas digitales o páginas web aplican medidas preventivas para evitar ataques de denegación de servicio (DDos). Esas organizaciones también implementan sistemas cortafuegos (firewalls) y algunas instituciones han implementado sistemas de detección y prevención de intrusiones; sin embargo, esto no se generalizó ni se implementó de manera consistente.

356. En el EGSI Versión 2.0, que es de aplicación obligatoria para instituciones de la administración pública central, se establecen una serie de controles, que incluyen controles y políticas de acceso (técnicas y físicas), gestión de acceso y responsabilidad de los usuarios, control de acceso a sistemas y aplicaciones, controles contra malware, implementación de respaldos de la información, control del software en producción, etc. Sin embargo, no todas las instituciones públicas obligadas están en un nivel de implementación del cien por ciento, lo cual genera la duda de si todos esos controles están siendo implementados.

357. También se mencionó que, el estándar NTE INEN-ISO/IEC 27002 adoptado por el Servicio Ecuatoriano de Normalización, es una norma técnica ecuatoriana que contiene una serie de controles técnicos de seguridad; sin embargo, no es de cumplimiento obligatorio para todas las instituciones públicas y organizaciones privadas.

358. En el sector financiero y de telecomunicaciones no se especificó la cantidad y naturaleza de los controles de seguridad técnica que las entidades reguladas deben implementar, y que son auditados por ARCOTEL y la Superintendencia de Bancos.

359. También se indicó que, algunos de los proveedores de servicios en Internet (e.g., Movistar) proveen servicios seguridad como parte de su cartera de servicios y además estos proveedores reconocen la necesidad de establecer políticas internas que incluyan la implementación de controles técnicos de seguridad para gestionar los riesgos identificados en los productos y servicios que ofrecen.

360. Se indicó que, en Ecuador, los controles criptográficos para proteger los datos en reposo y en tránsito son reconocidos e implementados por la mayoría de las instituciones públicas – principalmente por aquellas obligadas a cumplir con el EGSI vo2, control 6- y las organizaciones privadas que implementan estándares y buenas prácticas de seguridad internacionalmente reconocidas, especialmente el estándar ISO 27.001. Sin embargo, su uso aún no ha sido generalizado en todos los ambientes tecnológicos. La causa de esto puede ser el desconocimiento, la resistencia de adopción de nuevas tecnologías, sistemas obsoletos a los cuales no se les puede adaptar estos controles criptográficos y de cifrado, y la falta de socialización de estas herramientas.

361. También se comentó que, con la masificación del teletrabajo en los últimos dos años, instituciones públicas y organizaciones privadas han difundido ampliamente el uso de la Firma Digital y Virtual Private Network (VPNs) -para comunicaciones más seguras. Sin embargo, el nivel de conciencia de transferir información de forma cifrada aún debe de mejorar, ya que todavía se transfiere información sensible por medio del File Transfer Protocol, el cual es considerado un protocolo inseguro, según se indicó.

362. También se mencionó que, con la entrada en vigor de la LOPDP y su reglamento (todavía en pendiente) tanto las instituciones públicas como las organizaciones privadas deberán implementar protocolos y controles criptográficos más robustos a efectos de proteger los datos personales que tratan.

363. La mayoría de los portales y páginas web del Gobierno usan el protocolo Transport Layer Security (TLS), aunque no todas usan la última versión de seguridad TLS 1.3. Por ejemplo, las páginas web de MINTEL, MDN, Presidencia, Migración, Gobierno Electrónico, entre otros, usan la versión de seguridad TLS 1.3., mientras que portales como Gob.ec y la página web del Ministerio de Trabajo usan la versión TLS 1.2., lo cual se puede mejorar implementando la versión TLS 1.3.

364. En el caso del sector privado, el uso protocolos de seguridad TLS 1.3 es más avanzado. Se hizo un análisis entre una variedad de empresas locales y la mayoría usan la versión de seguridad más reciente, TLS 1.3. También se hizo una revisión de los portales o páginas web de las 5 empresas más importante de Ecuador, según un ranking empresarial, y solo 2 utilizan la versión TLS 1.3., las otras 3, usan la versión anterior -TLS 1.2, incluyendo un banco y un operador de telecomunicaciones.

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

D 5.3 CALIDAD DEL SOFTWARE

Nivel de Madurez: Formativo a Establecido

365. En términos generales, los requerimientos funcionales y de calidad del software en los sectores públicos y privados son reconocidos e identificados, pero no necesariamente de una forma estratégica.

366. Como se comentó arriba, el Portal Único de Software Ecuatoriano, es el catálogo único de la oferta de software de cualquier modalidad con valor agregado ecuatoriano mayoritario e importante e integra la información contenida en el catálogo de software publicado en el Sistema de Información de Ciencia, Tecnología, Innovación y Saberes Ancestrales y el catálogo de la oferta nacional de software. Como parte de los criterios del justificativo, según el orden de prelación, MINTEL evaluará varios parámetros, entre ellos los estándares de seguridad, que podría incluir una auditoría del código fuente, el soporte técnico, costo de oportunidad y la sostenibilidad de la solución (art. 10 del Decreto No. 1073).

367. Según los parámetros de uso e implementación de estándares de seguridad para las tecnológicas de la información y comunicación en los sectores público y privado, se determinó que una buena parte de las instituciones públicas y organizaciones privadas tienen políticas y procesos para la actualización y mantenimiento del software, pero no de forma consistente en todos los sectores. Para las instituciones públicas obligadas a cumplir el EGSI vo2, existen controles específicos en el ámbito de las actualizaciones y mantenimiento de software.

368. Aunque aparentemente MINTEL si lo realiza (art. 11 del Decreto No. 1073), no quedó claro en las sesiones virtuales, si las deficiencias de la calidad del software son recopiladas y evaluadas para determinar su impacto en la usabilidad y rendimiento.

369. En el sector financiero, la norma técnica de riesgo operativo de la Superintendencia de Bancos establece una serie de estándares y requerimientos de calidad del software; sin embargo, son incorporadas de forma paulatina en los desarrollos nuevos, ya que se deben hacer inversiones planificadas para la implementación de soluciones tecnológicas que permitan efectuar una gestión de calidad del software de forma eficiente, caso contrario se requiere contar con personal suficiente para realizar dichas acciones.

Este Factor evalúa la existencia de infraestructura y servicios de Internet confiables en el país, así como la existencia de 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 las redes y los sistemas son subcontratadas.

D 5.4 RESILIENCIA DE LA INFRAESTRUCTURA DE INTERNET Y DE LAS COMUNICACIONES

Nivel de Madurez: Formativo a Establecido

370. Un reporte del Banco Interamericano de Desarrollo indicó que Ecuador todavía tiene un camino importante por delante en el fortalecimiento de la conectividad digital. La penetración de los servicios de Banda Ancha (BA) fija y móvil es tan solo un 10 % y un 53 %, respectivamente, por debajo del resto de países de ALC (13 % y 65 %) y muy lejos de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) (33 % y 96 %). Tan sólo el 62 % de la población está cubierta por redes de BA móvil de alta velocidad (vs. 67 % en ALC y 98 % en la OCDE).

371. En el año 2021, varios medios de comunicación publicaron la noticia de que El internet en Ecuador "resulta muy caro y poco eficiente". Ecuador es el segundo país de Sudamérica, luego de Bolivia, con las tarifas menos accesibles para la contratación del servicio de internet de banda ancha fija y, además, la conexión es lenta e ineficiente. Según indicó el señor Carlos Zaldumbide, director ejecutivo de la Cámara de Comercio de Quito, con motivo del lanzamiento de la "Estrategia Nacional de Comercio Electrónico", que en dicha estrategia no hay una ruta clara para incrementar y fortalecer la infraestructura de conectividad en el país, así que, si el servicio de internet fijo no mejora en calidad, precios accesibles, y mayor cobertura, resultará complicado lograr los objetivos de esa estrategia.

372. Se determinó que, Ecuador tiene varias políticas públicas para mejorar la conectividad de banda ancha en todo el país e incluso para mejorar la dinámica del comercio electrónico; sin embargo, varios participantes mencionaron que todavía no existe una conectividad totalmente estable, confiable y asequible y que es un tema que las autoridades competentes (ARCOTEL, MINTEL, etc.) deben resolver.

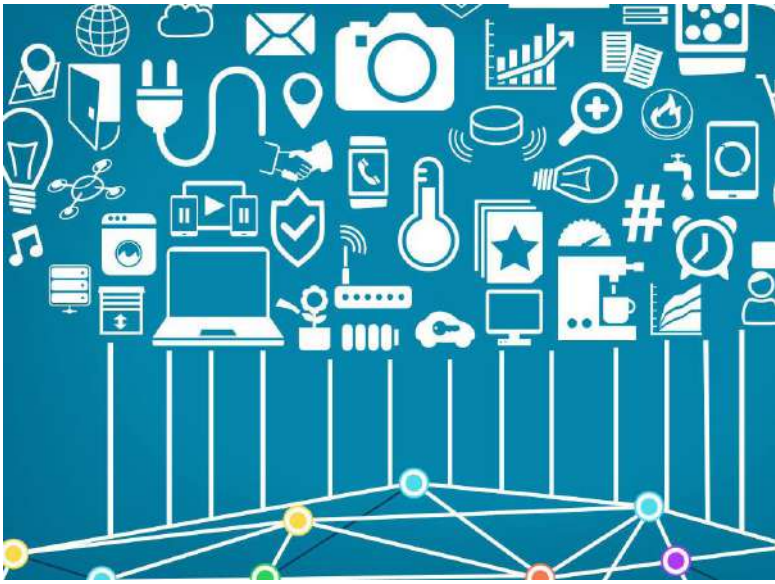
373. También se indicó que las tecnologías implementadas y los procesos usados para gestionar la infraestructura de Internet cumplen con estándares y buenas prácticas internacionales. Así mismo, que la infraestructura nacional es gestionada y administrada mediante procesos debidamente documentados, y las autoridades competentes (MINTEL, ARCOTEL, etc.) tienen total claridad de sus funciones y responsabilidades. Para tales efectos, ARCOTEL ha emitido normas técnicas y resoluciones para garantizar la calidad de los servicios de telecomunicaciones, incluyendo el servicio de Internet, tanto fijo y como móvil.

374. También se indicó que el Internet en Ecuador es ampliamente usado para hacer compras por Internet, transacciones comerciales electrónicas y otras transacciones, como pago de servicios, banca electrónica, etc. Producto de la pandemia, el comercio electrónico en Ecuador alcanzó un volumen de negocio de USD 2.3 mil millones, lo que supone un crecimiento de USD 700 millones (43,75 %) frente al 2019. Se estima que ese crecimiento continuará por los próximos años.

375. En varias sesiones virtuales se determinó que, la mayoría de los operadores de telecomunicaciones en Ecuador manejan un nivel de conciencia importante sobre los temas de ciberseguridad, además varios son empresas transnacionales. Por tal motivo, estos operadores implementan políticas de seguridad de conformidad con estándares de seguridad internacionales, lo cual incluye la evaluación de los riesgos cibernéticos como parte de la evaluación general de riesgos.

376. En varias sesiones virtuales se determinó que, tanto en el sector público (e.g., EGSI Versión 2.0) como en el sector privado se implementan políticas y protocolos de seguridad que están basadas en un enfoque de gestión de riesgos y se ejecutan evaluaciones de riesgos, ponen a prueba el nivel de resiliencia de las redes y cuentan con recursos internos y externos para gestionar el ciclo de respuesta a incidentes. Se estima que la mayoría de las PYMES todavía no tienen esa capacidad, aunque los servicios SOC son asequibles incluso para ese segmento empresarial.

377. También se determinó que la mayoría de las instituciones públicas (EGSI Versión 2.0) y privadas tienen algún tipo de mecanismos o plan de respuesta a incidentes que regularmente son puestos a prueba mediante simuladros y están bajo constante revisión. A menos que sea una empresa grande o transnacional, no todas las organizaciones cuentan con los recursos suficientes para atender todas y cada una de las siguientes actividades: integración de hardware, pruebas de estrés de software y tecnológico, capacitación de personal, monitoreo y respuesta a incidentes, y simulacros para poner a prueba los planes o protocolos de respuesta a incidentes.



D 5.5 MERCADO DE CIBERSEGURIDAD

Nivel de Madurez: Formativo a Establecido

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

378. Se informó que Ecuador tiene un mercado de productos y servicios de ciberseguridad pequeño e incipiente, pero activo. En el sector de servicios, se determinó que existen varios proveedores de servicios de ciberseguridad. En el sector de productos, al parecer todavía no se diseñan y desarrollan productos de ciberseguridad en el país, pero varias empresas ofrecen productos de ciberseguridad de empresas internacionales, entre ellos, cortafuegos, antivirus y otras herramientas especializadas para mitigar las vulnerabilidades de ciberseguridad, como productos para prevenir los ataques tipo DDoS.

379. Durante el presente diagnóstico se determinó que, los proveedores de tecnologías de ciberseguridad entienden y reconocen la necesidad de adoptar políticas y procesos seguros durante la etapa de desarrollo, pero no en todos los casos, esos procesos y políticas han alcanzado un nivel operativo. En el caso de productos importados de tecnología de ciberseguridad, la mayoría de los actores del ecosistema entienden que se deben analizar las implicaciones de seguridad, pero no siempre se cuenta con los recursos para tomar las medidas de mitigación que normalmente son ejecutadas dentro de un contexto de cadena de distribución internacional.

380. En Ecuador existen cada vez más consultores independientes y empresas consultoras que ofrecen servicios de consultoría en temas de ciberseguridad tanto para las instituciones públicas como para las organizaciones privadas. No es claro si las empresas existentes son suficientes para atender la demanda del mercado local. En virtud de que existen pocos profesionales en seguridad con certificaciones de la industria, y donde incluso la demanda por los servicios de este tipo de profesionales va en crecimiento, varias de estas empresas consultoras proporcionan información de su staff en las páginas web u otros medios (e.g, redes sociales). También se comentó que, actualmente, las consultorías en temas de seguridad Informática para redes IT/OT, por el desarrollo de Industrias 4.0, y la adopción de Internet of Things (IoT) han crecido sustancialmente en los últimos 2 años.

381. También se determinó que, no existe ningún tipo de guía, registro de profesionales dentro de colegios profesionales afines -que según se informó los mismos fueron eliminados por ley- y/o grupos o asociaciones gremiales que brinden asesoría y asistencia en el proceso de selección de estas empresas consultoras. Pese a lo anterior, se informó que dentro del portal del EcuCERT existe un listado de CERT públicos y privados que ofrecen ciertos servicios a la comunidad. También se mencionó que existen páginas web locales que contienen listas de empresas de seguridad y de profesionales en seguridad.

382. Como se indicó arriba, la mayoría de las instituciones más importantes dentro de los sectores público y privado realizan evaluaciones de riesgos, incluyendo el análisis de los riesgos cibernéticos, para determinar cómo se mitigan los riesgos relacionados con la subcontratación de tecnologías de la información o servicios en la nube.

383. En Ecuador existe un amplio entendimiento a nivel de las organizaciones sobre las garantías de seguridad que

brindan los proveedores de servicios IT subcontratados. Así mismo, un segmento amplio de organizaciones de los sectores público y privado han desarrollado y probado los procesos y protocolos orientados a garantizar la continuidad del negocio y la recuperación de la operación ante desastres.

384. Varios participantes informaron que, en Ecuador ya existe un mercado incipiente de ciberseguros a nivel corporativo. Ciertas organizaciones grandes y/o transnacionales, como bancos e instituciones financieras principalmente, han adoptado la buena práctica de adquirir este tipo de seguro. Se informó que este tipo de seguros tienen coberturas según las necesidades del asegurado, cubren riesgos sobre la interrupción de las actividades medulares de la operación, el reembolso de los gastos incurridos en la recuperación de la información, así como sus responsabilidades derivadas de ello. No se pudo determinar si existen opciones de ciberseguros en el mercado ecuatoriano que se ajusten a las necesidades y posibilidades de las PYMES.

385. También se identificó que, en Ecuador existe un seguro corporativo que cubre equipos electrónicos, específicamente contra todo riesgo de daño accidental, incendio, explosión, robo y/o asalto, daños materiales causados a los equipos electrónicos, etc.

386. En la presente revisión se determinó que, una aseguradora regional con operación en Ecuador ofrece un tipo de seguro denominado como seguros informáticos, cibernéticos o de internet, que se dividen en una amplia gama de posibles seguros, tales como seguro por difamación, plagio de ideas, violación de derechos de autor, divulgación no autorizada de información, robo de datos, pérdida de datos personales, extorsión comercial, violaciones de seguridad y privacidad, transmisión de virus informáticos, entre otros.

D 5.6 DIVULGACIÓN RESPONSABLE DE VULNERABILIDADES

Este Factor evalúa el establecimiento de un marco regulatorio referente a la divulgación responsable para la recepción y difusión de información de vulnerabilidades y otros incidentes en todos los sectores, y si además existe la capacidad para revisar y actualizar continuamente este marco regulatorio.

Nivel de Madurez: Formativo

387. En Ecuador todavía no existe un marco legal o regulatorio, de aplicación nacional, que obligue a las instituciones públicas y organizaciones privadas a divulgar las vulnerabilidades, errores y fallas de seguridad y/o a compartir información de incidentes, vulnerabilidades, etc. Debido a lo anterior, tampoco existen mecanismos de protección legal en el ámbito de divulgación responsable de vulnerabilidades. Los participantes del sector público y privados entienden y reconocen la necesidad de establecer mecanismos ágiles para reportar vulnerabilidades y otras fallas de seguridad, así como plataformas con protocolos formales para compartir información a nivel nacional y sectorial.

388. En el sector público, el EGSI Versión 2.0 establece una serie de disposiciones son respecto a la gestión de vulnerabilidades (control 8) y a la gestión de incidentes de seguridad informática (control 12), los cuales deben reportarse a las autoridades competentes, MINTEL y EcuCert, en el tiempo y forma indicados.

389. A nivel sectorial, específicamente en el sector de telecomunicaciones, existe una norma técnica de gestión de incidentes y vulnerabilidades (ver D1.2), la cual establece que las notificaciones deben enviarse a ARCOTEL a través de un correo electrónico de EcuCERT, y luego ARCOTEL notificará a los operadores que puedan verse afectados. También esa norma técnica establece los protocolos de confidencialidad para el intercambio de información y los tiempos de recepción, gestión y respuesta de notificaciones tanto para incidentes como para vulnerabilidades.

390. En el sector financiero u otros sectores críticos o esenciales tampoco se identificó algún tipo de norma técnica o resolución con respecto a la divulgación responsable de vulnerabilidades e incluso intercambio de infor-

mación; sin embargo, en aquellos servicios que son regulados, los proveedores del servicio tienen la obligación de notificar al ente regulador los incidentes que interrumpan la disponibilidad y continuidad del servicio, entre ellos, los incidentes cibernéticos.

391. Debido a que en Ecuador existe una dependencia por productos tecnológicos y de ciberseguridad de proveedores internacionales, estos una vez reportados, ya sea localmente o por otros medios, son remediados de forma expedita y los usuarios son notificados para realizar las actualizaciones pertinentes. En cuanto a los servicios de ciberseguridad que se ofrecen las empresas locales, estas también tienen un tiempo de resolución bastante rápido.

392. En el ámbito de intercambio de información, si existen varios mecanismos que funcionan formal o informalmente en Ecuador. Por ejemplo, los dos mecanismos que gestiona el EcuCERT (ver D1.2).

393. Por medio de la página web del EcuCERT los operadores de telecomunicaciones y el público en general pueden reportar los incidentes cibernéticos en el siguiente enlace https://www.ecucert.gob.ec/incidentes/. Así mismo, el EcuCERT también pone a disposición otros mecanismos para reportar de incidentes, tales como una llamada telefónica, reportes directamente en la oficina, reportes vía email, etc.

394. En el portal único de trámites de ciudadanos (Gob.ec) se proporciona información sobre el reporte de incidentes cibernéticos en las redes de telecomunicaciones y los mecanismos disponibles para realizar los reportes a ARCOTEL a través del EcuCERT.

395. También se indicó que, los CERT públicos y privados tienen varios mecanismos de reporte de incidentes exclusivos para las organizaciones de su comunidad objetivo. En algunos CERTs esos mecanismos no están disponibles para el público en general, mientras que en otros el público en general puede reportar los incidentes por esos medios, información que luego es compartida con el EcuCERT y otras entidades competentes.

RECOMENDACIONES

Después de analizar la evidencia presentada y recopilada durante los grupos focales con respecto a los estándares y tecnologías de ciberseguridad, se realizan las siguientes recomendaciones a Ecuador. Estas recomendaciones tienen como objetivo proporcionar consejos y pasos a seguir para mejorar la capacidad de ciberseguridad existente, siguiendo las consideraciones del modelo del CMM.

CUMPLIMIENTO DE ESTANDARES

R5.1 Desarrollar e implementar un esquema nacional de seguridad de la información (ENSI) basado en estándares y buenas prácticas internacionales de seguridad, el cual será de cumplimiento (voluntario u obligatorio, según se acuerde) para las organizaciones de los sectores público y privado.

R5.2 Asegurarse que el ENSI contemple mecanismos de control y estándares de seguridad relacionados con las TICs, a los procesos de adquisición de software, hardware, tercerización de servicios y servicios cloud, y a la provisión de productos y servicios.

R5.3 Designar a una agencia de gobierno (e.g., MINTEL) o un comité que se encargue de la implementación, auditoría y medición de cumplimiento del ENSI en los sectores público y privado. Que dicho ente rector recopile métricas y estadísticas que informen el proceso de cumplimiento y la asignación de recursos. Así mismo, que dicho ente realice periódicamente auditorías.

R5.4 Promover debates sobre cómo se pueden utilizar los estándares y las buenas prácticas de seguridad para abordar los riesgos cibernéticos en las cadenas de suministro de las IC, por parte de organizaciones gubernamentales y operadores de IC tanto públicos

como privados. Identificar y exigir estándares y buenas prácticas de seguridad a todos los proveedores de IC.

R5.5 Revisar periódicamente tanto los controles y estándares de seguridad del EGSI Versión 2.0 como su proceso de implementación con el fin de realizar las actualizaciones necesarias de conformidad con los requerimientos y prioridades del sector público. Así mismo, considerar la posibilidad de que la aplicación del EGSI Versión 2.0 se extienda a todas las instituciones del sector público, incluyendo gobiernos locales.

R5.6 Asegurarse que MINTEL como responsable de la implementación, auditoría y medición del EGSI vo2 tenga los recursos necesarios para auditar periódicamente a las instituciones obligadas y supervisar el cumplimiento del EGSI vo2 - y que además fortalezca los mecanismos de recopilación de métricas y estadísticas sobre el proceso de cumplimiento.

R5.7 Asegurarse que todas instituciones obligadas al EGSI vo2 logren el cien por ciento de cumpliendo dentro del plazo establecido por MINTEL. Así mismo, darle los recursos necesarios a los CISOs de las instituciones obligadas para cumplir con ese cometido y que además la implementación del EGSI vo2 se convierta en un proceso estructurado, sistemático y continuo.

R5.8 Establecer un régimen sancionatorio administrativo para los casos de incumplimiento del EGSI vo2 y del ENSI de conformidad con los modelos de gobernanza y cumplimiento establecidos.

R5.9 Promover el conocimiento y la implementación de estándares de seguridad entre las PYMES.

CONTROLES DE SEGURIDAD

R5.10 Implementar controles técnicos de seguridad actualizados, tales como parches de software y respaldo o copias de seguridad, y controles físicos de seguridad, para prevenir accesos no autorizados en las instalaciones computacionales, en todos los sectores del ecosistema.

R5.11 Establecer políticas internas para la implementación de controles técnicos de seguridad -basados en estándares y buenas prácticas internacionales - tanto en el sector público como el sector privado, incluyendo proveedores de IC y proveedores de servicios de Internet y otras tecnologías. Supervisar periódicamente el uso de estos controles y revisar los resultados para mejorar su implementación.

R5.12 Fomentar el desarrollo y la difusión de controles criptográficos en todos los sectores y usuarios para la protección de datos en reposo y en tránsito, de conformidad con los estándares y buenas prácticas internacionales.

R5.13 Generar conciencia en todos los sectores sobre los servicios de comunicación segura, tales como correos electrónicos encriptados/firmados electrónicamente.

R5.14 Implementar técnicas robustas de cifrado en los datos -en reposo – de los data centers.

R5.15 Promover la implementación de herramientas de última generación, como SSL o TLS, por parte de los proveedores de servicios web, para asegurar todas las comunicaciones entre servidores y navegadores web. Lo anterior no solo debe dirigirse a los proveedores de servicios, sino también a las organizaciones públicas y privadas, en particular a las PYMES, para que soliciten la implementación de esas herramientas a sus proveedores de servicios.

CALIDAD DEL SOFTWARE

R5.16 Desarrollar y/o actualizar periódicamente los catálogos de plataformas y aplicaciones de software seguras, incluyendo los requerimientos de calidad y funcionales, que sean aplicables a los sectores público y privado, en particular a los proveedores de IC o servicios esenciales. Así mismo, garantizar que esas plataformas y aplicaciones de software seguras cumplen con los estándares y buenas prácticas internacionales.

R5.17 Asegurarse que las organizaciones de los sectores público y privado implementan procesos y políticas internas para la actualización y mantenimiento (gestión de parcheo) del software.

R5.18 Desarrollar y/o actualizar periódicamente el inventario de software y aplicaciones seguras utilizadas en el sector público.

R5.19 Asegurarse que dichas plataformas y aplicaciones de software sean reconocidas por su confiabilidad, usabilidad y desempeño de conformidad con los estándares y buenas prácticas internacionales. Así mismo, evaluar la evidencia de las deficiencias en la calidad del software con respecto a su impacto en la confiabilidad, usabilidad y el rendimiento.

RESILIENCIA DE LA INFRAESTRUCTURA DE INTERNET Y DE LAS COMUNICACIONES

R5.20 Revisar la disponibilidad y fiabilidad del servicio de Internet en todas las regiones del país. Así mismo, identificar y mapear los puntos de fallas críticas dentro de la infraestructura de Internet.

R5.21 Evaluar periódicamente si los procesos y las tecnologías empleadas para la administración de la infraestructura de Internet cumplen con las normas regulatorias locales y los estándares y buenas prácticas internacionales.

R5.22 Garantizar que todos los procesos utilizados para administrar y monitorear la infraestructura nacional están documentados, los gestores tienen funciones y responsabilidades definidas y existe en el país una redundancia adecuada.

R5.23 Mejorar la coordinación con respecto a la resiliencia de la infraestructura de Internet en los sectores público y privado.

R5.24 Asegurarse que todas las organizaciones públicas y privadas realizan evaluaciones de riesgo cibernético y tienen los mecanismos para monitorear y poner a prueba la resiliencia de las redes. También asegurarse que dichas organizaciones cuentan con planes, mecanismos y procesos para gestionar la respuesta a incidentes cibernéticos, lo cual incluye recursos tecnológicos y financieros y capital humano calificado para esos fines.

MERCADO DE CIBERSEGURIDAD

R5.25 Promover la producción y comercialización de productos innovadores de ciberseguridad por parte de empresas tecnológicas nacionales, tanto para uso y consumo local como para exportación.

R5.26 Asegurarse que los productos tecnológicos y de ciberseguridad importados cumplen con los estándares y buenas prácticas internacionales en el ámbito de la cadena de suministros.

R5.27 Promover el uso de lineamientos, buenas prácticas y estándares internacionales de codificación segura para el desarrollo de software en el país.

R5.28 Asegurarse que todas las organizaciones de los sectores público y privado realizan evaluaciones de riesgo para determinar cómo mitigar los riesgos asociados con la subcontratación de servicios IT o servicios cloud. Así mismo, que existe una comprensión generalizada de las garantías de seguridad proporcionadas por los proveedores de esos servicios.

R5.29 Asegurarse que la mayoría de las organizaciones de los sectores público y privado han desarrollado y puesto a prueba planes y procesos para garantizar tanto la continuidad del negocio como la recuperación ante desastres o crisis.

R5.30 Promover y consolidar el mercado de seguros cibernéticos en el país y alentar el intercambio de información entre los participantes del mercado. Así mismo, asegurarse que existen opciones de pólizas para las PYMES.

DIVULGACIÓN RESPONSABLE DE VULNERABILIDADES

R5.31 Establecer un marco legal o regulatorio, de aplicación nacional, que obligue a las instituciones públicas y organizaciones privadas a divulgar de forma responsable y coordinada las vulnerabilidades, errores y fallas de seguridad y/o a compartir información de incidentes, vulnerabilidades, etc. Así mismo, que ese marco establezca las actividades que podrán y no podrán ejecutar los denunciantes, plazos límite de divulgación y resolución (parcheo y actualizaciones), mecanismos de coordinación con proveedores, mecanismos de divulgación hacia la comunidad, y mecanismos de protección legal y reconocimiento para los denunciantes de buena fe.

R5.32 Nombrar a un ente responsable de la supervisión del cumplimiento de los procedimientos de divulgación responsable arriba indicados y que garantizarse que los proveedores no oculten información relacionada con la vulnerabilidad, error y/o falla de seguridad.

R5.33 Asegurarse que los proveedores de productos tecnológicos y de ciberseguridad locales también tienen un protocolo para recibir, solucionar y diseminar la información sobre vulnerabilidades.

R5.34 Desarrollar un sistema o plataforma que facilite el intercambio de inteligencia sobre amenazas, vulnerabilidades, etc. entre todos los actores del ecosistema.

R5.35 Fortalecer los mecanismos existentes de notificación de incidentes en el sector público y promover su uso.

R5.36 Definir umbrales y requisitos de notificación para todos los sectores. Estos requisitos no solo deben considerar la disponibilidad de los servicios, sino también la integridad y confidencialidad de los datos.

REFLEXIÓN FINAL

396. El equipo de revisión del CMM y el Banco Mundial agradecen al Ministerio de Telecomunicaciones y de la Sociedad de la Información, al Comité Nacional de Ciberseguridad de Ecuador y al EcuCERT por el excelente apoyo brindado durante la preparación, implementación y seguimiento de la presente evaluación, así como a todas las partes interesadas que asistieron a las sesiones presenciales y virtuales. La organización, representación y composición de los grupos participantes fue integral y equilibrada, y todos ofrecieron contribuciones positivas y que fueron de mucha utilidad para generar el presente reporte, el cual muestra una radiografía del estado de situación de la ciberseguridad en Ecuador. Así mismo, se notó que el Gobierno de Ecuador claramente está dándole el nivel de prioridad a los temas ciberseguridad, y se espera que los actores del ecosistema encuentren útiles las observaciones y recomendaciones del presente informe.

BIBLIOGRAFÍA

1. Cybersecurity Capacity Maturity Model for Nations (CMM), Edición 2021, https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf (revisado el día 22 de noviembre del 2022).
2. Relevant publications: Williams, M. (2003). Making Sense of Social Research. Sage Publications: London; Knodel, J. (1993). "The Design and Analysis of Focus Group Studies: A Practical Approach". in Successful focus groups: Advancing the state of the art. Morgan, D. L. (Ed.). SAGE Publications: Thousand Oaks, CA; Krueger, R.A. and Casey, M.A. (2009). Focus Groups: A Practical Guide for Applied Research. Sage Publications: London.
3. Relevant publications: Kitzinger, J. (1994). "The Methodology of Focus Groups: The Importance of Interaction between Research Participants. "Sociology of Health & Illness, 16(1). Disponible en https://doi.org/10.1111/1467-9566.ep11347023 (revisado el día 22 de noviembre del 2022); Kitzinger, J. (1995). "Qualitative Research: Introducing Focus Groups". British Medical Journal, 311(7000). Disponible en https://doi.org/10.1136/bmj.311.7000.299 (revisado el día 22 de noviembre del 2022); Fern, E.F. (1982). "The Use of Focus Groups for Idea Generation: The Effects of Group Size, Acquaintanceship, and Moderator on Response Quantity and Quality".Journal of Marketing Research, 19(1). Disponible en https://doi.org/10.1177%2F002224378201900101 (revisado el día 22 de noviembre del 2022).
4. Kitzinger, J. (1995).
5. Krippendorff, K. (2004). Content Analysis: An Introduction to its Methodology. Sage Publications: Thousand Oaks, CA; Hsieh, H.F. and Shannon, S.E. (2005). "Three Approaches to Qualitative Content Analysis." Qualitative Health Research, 15(9). Disponible en https://journals.sagepub.com/doi/pdf/10.1177/1049732305276687 (revisado el día 22 de noviembre del 2022); Neuendorf, K.A. (2002). The Content Analysis Guidebook. Sage Publications: Thousand Oaks, CA.
6. Fern, E.F. (1982).
7. Elo, S. and Kyngäs, H. (2008). "The Qualitative Content Analysis Process."Journal of Advanced Nursing, 62(1). Disponible en https://doi.org/10.1111/j.1365-2648.2007.04569.x (revisado el día 22 de noviembre del 2022); H.F. and Shannon, S.E. (2005).
8. Downe-Wamboldt, B. (1992). "Content Analysis: Method, Applications, and Issues."Health Care for Women International, 13(3). Disponible en https://doi.org/10.1080/07399339209516006 (revisado el día 22 de noviembre del 2022).
9. Dey, I. (1993). Qualitative Data Analysis: A User-friendly Guide for Social Scientists. Routledge: London.
10. Landeta, D. (n.d.). La demanda de Internet subió 30% durante la emergencia. El Comercio. Revisado el día 22 de noviembre del 2022. Disponible en https://www.elcomercio.com/actualidad/negocios/demanda-internet-emergencia-coronavirus-ecuador.html
11. La pandemia incrementó la demanda de Internet en un 40%. (n.d.). Revistalideres.Com. Revisado el día 22 de noviembre del 2022, disponible en https://www.revistalideres.ec/lideres/informe-educacion-comercio-pandemia-internet.html
12. Abonados y usuarios – Agencia de Regulación y Control de las Telecomunicaciones. (n.d.). Revisado el día 22 de noviembre del 2022, disponible en https://www.arcotel.gob.ec/abonados-y-usuarios/
13. Ecuador: Avance en el sector telco mientras la TV Paga sigue en descenso y continúa la piratería. (n.d.). Televisión. Revisado el día 22 de noviembre del 2022, disponible en https://www.prensario.net/37242-Ecuador-Avance-en-el-sector-telco-mientras-la-TV-Paga-sigue-en-descenso-y-continua-la-pirateria.note.aspx
14. Landeta, D. (n.d.). La demanda de Internet subió 30% durante la emergencia. El Comercio. Revisado el día 22 de noviembre del 2022, disponible en https://www.elcomercio.com/actualidad/negocios/demanda-internet-emergencia-coronavirus-ecuador.html

15. El MINTEL destaca el aporte de las TIC frente al COVID-19 – Ministerio de Telecomunicaciones y de la Sociedad de la Información. (n.d.). Revisado el día 22 de noviembre del 2022, disponible en https://www.telecomunicaciones.gob.ec/el-mintel-destaca-el-aporte-de-las-tic-frente-al-covid-19/ /
16. Landeta, D. (n.d.). La demanda de Internet subió 30% durante la emergencia. El Comercio. Revisado el día 22 de noviembre del 2022, disponible en https://www.elcomercio.com/actualidad/negocios/demanda-internet-emergencia-coronavirus-ecuador.html /
17. Ortiz, D. (2021). Ecuador está entre los países con más ciberataques en América Latina. El Comercio. Revisado el día 22 de noviembre del 2022, disponible en https://www.elcomercio.com/tendencias/tecnologia/ecuador-ciberataques-america-latina-hacker.html
18. Ver https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
19. El MINTEL suscribió con Cyber4Dev, proyecto de la Unión Europea, un Memorando de Entendimiento para fortalecer la ciberseguridad en Ecuador – Ministerio de Telecomunicaciones y de la Sociedad de la Información. (n.d.). Revisado el día 22 de noviembre del 2022, disponible https://www.telecomunicaciones.gob.ec/el-mintel-suscribio-con-cyber4dev-proyecto-de-la-union-europea-un-memorando-de-entendimiento-para-fortalecer-la-ciberseguridad-en-ecuador/
20. Capacitaciones – Proyecto Puntos del Encuentro. (n.d.). Revisado el día 22 de noviembre del 2022, disponible en https://puntosdelencuentro.mintel.gob.ec/capacitaciones-infocentros/
21. "Habilidades Digitales" un aplicativo de autodiagnóstico que nació como iniciativa del MINTEL – Ministerio de Telecomunicaciones y de la Sociedad de la Información. (n.d.). Revisado el día 22 de noviembre del 2022, disponible en https://www.telecomunicaciones.gob.ec/habilidades-digitales-aplicativo-autodiagnostico-nacio-iniciativa-del-mintel/
22. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/05/Agenda-Digital-del-Ecuador-2021-2022-222-comprimido.pdf
23. (N.d.). Twitter. Revisado el día 22 de noviembre del 2022, disponible en https://twitter.com/Educacion_Ec/status/1452736528392802306
24. 24, F. (2021). Las noticias falsas proliferan en la elección presidencial de Ecuador. France 24. Revisado el día 22 de noviembre del 2022, disponible en https://www.france24.com/es/minuto-a-minuto/20210410-las-noticias-falsas-proliferan-en-la-elecci%C3%B3n-presidencial-de-ecuador
25. (N.d.). Revisado el día 22 de noviembre del 2022, disponible en http://cne.gob.ec/es/institucion/sala-de-prensa/noticias/5722-ecuador-expone-los-mecanismos-que-utilizo-para-combatir-la-desinformacion-en-procesos-electorales
26. House, F. (n.d.). Ecuador. Freedom House. Revisado el día 22 de noviembre del 2022, disponible en https://freedomhouse.org/country/ecuador/freedom-net/2021
27. Corroborar la información es un compromiso de todos – Ministerio de Telecomunicaciones y de la Sociedad de la Información. (n.d.). Revisado el día 22 de noviembre, 2022, disponible en https://www.telecomunicaciones.gob.ec/corroborar-la-informacion-es-un-compromiso-de-todos/
28. Fundamedios, C. (2021). La experiencia de Ecuador Verifica en la lucha contra la desinformación. Ecuador Verifica. Revisado el día 22 de noviembre del 2022, disponible en http://ecuadorverifica.org/2021/06/09/la-experiencia-de-la-coalicion-ecuador-verifica-en-la-lucha-contra-la-desinformacion-se-conocio-en-la-conferencia-de-rightscon-para-combatir-la-desinformacion-y-las-fake-news/
29. Banco Interamericano de Desarrollo (2021). Servicios Públicos y Gobierno Digital Durante la Pandemia. Revisado el día 28 de noviembre de 2022, disponible en https://publications.iadb.org/publications/spanish/document/Servicios-publicos-y-gobierno-digital-durante-la-pandemia-Perspectivas-de-los-ciudadanos-los-funcionarios-y-las-instituciones-publicas.pdf

30. Ibid.
31. Ibid.
32. Franco, P.T. (2022) Entre $ 2.760 millones y $ 3.220 millones movió, Por Lo Menos, El e-commerce en Ecuador en el 2021, Economía | Noticias | El Universo. El Universo. Revisado el día 28 de noviembre de 2022, disponible en https://www.eluniverso.com/noticias/economia/entre-2760-millones-y-3220-millones-movio-por-lo-menos-el-e-commerce-en-ecuador-en-el-2021-nota
33. Cámara Ecuatoriana de Comercio Electrónico (2021). Transacciones electrónicas en Ecuador durante el Covid-19. Revisado el día 28 de noviembre de 2022, disponible en https://cece.ec/wp-content/uploads/2020/06/Transacciones-electronicas-en-Ecuador-durante-el-Covid19.pdf
34. Ley de Comercio Electrónico. Revisado el día 28 de noviembre de 2022, disponible en https://www.gob.ec/regulaciones/2002-67-ley-comercio-electronico-firmas-mensajes-datos
35. E-commerce Institure (2017). Primer Estudio de Comercio Electrónico en Ecuador. Revisado el día 28 de noviembre de 2022, disponible en https://ecommerce.institute/se-presento-el-primer-estudio-de-comercio-electronico-en-el-pais-durante-el-ecommerce-day-ecuador-2017/
36. Lorena Naranjo Godoy (2021). La Autoridad de Protección de Datos Personales deberá trabajar en la generación de Confianza Digital. Revisado el día 28 de noviembre de 2022, disponible en https://www.telecomunicaciones.gob.ec/lorena-naranjo-godoy-la-autoridad-de-proteccion-de-datos-personales-debera-trabajar-en-la-generacion-de-confianza-digital/
37. Policía Nacional del Ecuador (2015). Delitos Informáticos o Ciberdelito. Revisado el día 28 de noviembre de 2022, disponible en https://www.policia.gob.ec/delitos-informaticos-o-ciberdelitos/
38. Ver https://policiajudicial.gob.ec/1800-delito/
39. Pimentel, Carolina (2021). Más De 600 Denuncias Por Delitos Cibernéticos Se Han Registrado En Ecuador En Lo Que Va Del 2021. Seguridad | Noticias | El Universo, El Universo. Revisado el día 28 de noviembre del 2022, disponible en https://www.eluniverso.com/noticias/seguridad/mas-de-600-denuncias-por-delitos-ciberneticos-se-han-registrado-en-ecuador-en-lo-que-va-del-2021-nota/.
40. Municipio de Quito (2021). En 2020 Hubo Más De 200.000 Alertas Sobre Explotación Sexual Infantil Desde Ecuador. Revisado el día 22 de noviembre de 2022, disponible en https://www.planv.com.ec/historias/sociedad/2020-hubo-mas-200000-alertas-sobre-explotacion-sexual-infantil-desde-ecuador.
41. Escuela Superior Politécnica del Litoral (2021). Revisado el día 28 de noviembre de 2022, disponible en https://www.fiec.espol.edu.ec/postgrados/doctorado/doctorado-en-ciencias-computacionales-aplicadas
42. Ver https://aportecivico.gobiernoelectronico.gob.ec/system/documents/attachments/000/000/011/original/58b9ab393399dc479d2fb43c7a305ff0de62ec96.PDF
43. Ibid.
44. WIPO Legislation Website. Revisado el día 22 de noviembre de 2022, disponible en https://wipolex.wipo.int/en/treaties/ShowResults?country_id=51C
45. Banco Interamericano de Desarrollo (2020). Estado Actual de las Telecomunicaciones y la Banda Ancha en Ecuador. Revisado el día 22 de noviembre de 2022, disponible en https://publications.iadb.org/es/estado-actual-de-las-telecomunicaciones-y-la-banda-ancha-en-ecuador
46. "Servicio De Internet En Ecuador Es Uno De Los Más Caros Y Peores." Diario La Hora Ecuador, Revisado el día 28 de noviembre de 2022, disponible en https://www.lahora.com.ec/pais/servicio-de-internet-en-ecuador-es-uno-de-los-mas-caros-y-peores/
47. Ekos Negocios. En 2021, El Comercio Electrónico Mantendrá Un Crecimiento Sostenido En Ecuador. Ekos Negocios, Ekos Negocios, 9 Feb. 2021. Revisado el día 28 de noviembre de 2022, disponible en https://www.ekosnegocios.com/articulo/en-2021-el-comercio-electronico-mantendra-un-crecimiento-sostenido-en-ecuador.
48. Ver https://www.segurosdelpichincha.com/blogs/tipos-de-seguro-en-ecuador.html
49. Ver https://www.ngs.com.ec/?page_id=11


EL BANCO MUNDIAL
BIRF • AIF

www.telecomunicaciones.gob.ec

Ministerio de Telecomunicaciones
y de la Sociedad de la Información

República
del Ecuador