PUBLICACIÓN No. 5 | SEPTIEMBRE 17 DE 2020 | BOGOTÁ - COLOMBIA

CÁPSULAS SOBRE Ciberseguridad

AL DÍA CON FELABAN

Panorama de la estrategia de ciberseguridad en LATAM

FIC
FRAUD INFORMATION CONTROL
by FELABAN

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

55 AÑOS
1965 - 2020

Panorama de la estrategia de ciberseguridad en LATAM

En nuestra primera publicación de las cápsulas de ciberseguridad, hicimos un ejercicio de aproximación a este término y concepto. En dicha edición, se repasaron algunos conceptos emitidos por diferentes organismos, como lo considerado por la norma técnica ISO 27.032; el concepto emitido por el Financial Stability Board; El instituto Nacional de estándares y tecnología del Departamento de los Estados Unidos; la academia desde las publicaciones de Otis y Lorents y por último y no menos imparta el Comité de Supervisión Bancaria de Basilea.

Desde dichas perspectivas y a manera de síntesis, se indicó que con un resumen de la definición de Ciberseguridad sería entonces: todas aquellas medidas que se toman bien sean por una persona o por una empresa, para proteger su información una vez se ha conectado al ciberespacio, para evitar que se le proporcionen ciber ataques que afecten la confidencialidad o integridad de dicha información en razón a diversas formas de fraude.

Ahora bien, desde la perspectiva nacional en la esfera estatal, este término cobra un nuevo concepto y valor. Desde la noción del estado, se cubre la ciberseguridad, dentro de la estrategia nacional de seguridad, la cual básicamente se traduce en cómo se protege a dicho estado/nación de las amenazas.

Sin embargo, en los últimos años, esto ha tenido una nueva concepción debido a la evolución de la tecnología y la conectividad. Las amenazas para el siglo XXI, se han transmutado desde el campo físico a un campo también cibernético, lo que implica que el estado debe contemplar la seguridad física y cibernética, considerando las amenazas que puedan afectar a la nación, desde los diferentes frentes: aspectos sociales, políticos, económicos, ecológicos, culturales, etc.

La ciberseguridad es un tópico que llegó a las esferas de seguridad nacional, la estabilidad social y correcto funcionamiento del andamiaje económico. Los programas, los servidores, los datos, y los dispositivos son una herramienta que van desde el bolsillo de cada ciudadano, hasta mega computadoras que controlan y monitorean la electricidad, las transacciones financieras y las cámaras de seguridad del tráfico. Los organismos de seguridad estatal, tales como la policía, el ejército, la inteligencia hoy por hoy han abierto divisiones y personal calificado para atender las amenazas a las que cada país está expuesto en este frente. En sentido se han construido estrategias, mecanismos de defensa y preservación del orden.

Hay que decir que tanto el concepto de ciberseguridad, como el de estrategias nacionales sobre la misma, son un algo que hoy está lejos de tener consensos entre los expertos. Hoy en día no existe un término unificado para la definición del término ciberseguridad, los países basándose en los diferentes niveles de exposición en el ciber espacio y las respectivas amenazas que puedan poner en riesgo los frentes mencionados anteriormente, personalizan la definición de la estrategia nacional de ciberseguridad. Esto dificulta calificar y categorizar las estrategias desarrolladas por los países. Por supuesto una evaluación es una labor mucho más compleja.

Para contextualizar, podemos tomar como ejemplo la definición de la estrategia nacional de ciberseguridad desde la posición de EEUU y de la Unión Europea:

Desde los Estados Unidos, donde se considera la estrategia en el documento publicado en 2018 por el Presidente Donald Trump, se encuentra: el éxito de la estrategia será considerada cuando las vulnerabilidades sean efectivamente manejadas a través la identificación y protección de las redes, sistemas, funciones y datos, como también la detección, resiliencia, respuesta y recuperación de incidentes, que puedan ser destructivos, perjudiciales o desestabilizadores provenientes de actividades cibernéticas, dirigidas contra estados unidos.[1]

Para esto, se definen 4 lineamientos:

1. Defender la patria protegiendo redes, sistemas, funciones y datos.
2. Promover la prosperidad nacional al fomentar seguridad, economía digital prospera, y la innovación nacional.
3. Preservar la paz y seguridad fortaleciendo la capacidad de los Estados Unidos (con aliados y socios), para disuadir y de ser necesario, castigar a quienes usen herramientas cibernéticas con fines maliciosos.
4. Expandir la influencia americana en el extranjero para extender los principios clave de una internet abierta, interoperable, confiable y segura. (White House, 2018).

La segunda, y en pleno contraste viene desde la Agencia de la Unión Europea para al Ciberseguridad (ENISA, por sus siglas en Inglés European Union Agency for Cybersecurity), se encuentra: contribuir con la política cibernética de la UE, mejorando la confiabilidad de los productos, servicios y procesos de TIC´s, con esquemas de certificación en ciberseguridad, cooperación con los estados miembros, y los organismos de la UE, para ayudar a Europa a prepararse para los desafíos cibernéticos, alcanzando altos niveles en común en términos de ciberseguridad en toda la Unión Europea en cooperación con la comunidad en general.

1. The White house, National Cyber Strategy, United States of America, 2018. En: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Definiendo los siguientes lineamientos:

1. Potenciar y conectar con comunidades a través de un ecosistema de ciberseguridad. Esto a través de una estrategia del estado del arte sobre conceptos y prácticas de ciberseguridad, que fomenten a cooperación entre actores claves y creando sinergias. Este ambiente cibernético, que empodere autoridades de los estados miembros de la UE, instituciones, agencias, organismos, asociaciones, centros de investigación, universidades, industrias, actores privados y ciudadanos, ya que todos juegan un rol importante en hacer a Europa ciber segura.

2. Ciberseguridad como una parte integral de las políticas de la UE. Asesorar y apoyar proactivamente a los actores relevantes de la UE, incorporando la dimensión de ciberseguridad en el desarrollo del ciclo de vida de las políticas, a través de directrices específicas viables y técnicas.

3. Cooperación efectiva entre actores operacionales dentro de la UE, en caso de incidentes cibernéticos masivos. Apoyo y cooperación transfronterizos entre miembros de los estados de la UE, ante posibles incidentes y crisis a gran escala. Apoyo a la ampliación técnica, operativa, política y estratégica entre actores para permitir una respuesta oportuna, intercambio de información, conocimiento de la situación y comunicación de crisis en toda la Unión. Además de un manejo técnico integral y rápido a solicitud de los estados miembros, para facilitar necesidades técnicas y operáticas en la gestión de incidentes y crisis.

4. Competencia de vanguardia y capacidades en ciberseguridad a través de la UE. Competencias alineadas en ciberseguridad, experiencia profesional y estructuras educativas para cumplir con las necesidades, cada vez mayores, de conocimientos y competencias en ciberseguridad en la UE, mientras se incorporan tecnologías cibernéticas. Así también, capacidades bien preparadas y probadas con capacidad adecuada para hacer frente a la evolución entorno de amenazas a la UE.

5. Alto nivel de confianza en asegurar soluciones digitales. El entorno digital ciberseguro en toda la UE, donde los ciudadanos pueden confiar en los productos, servicios y procesos de las TIC´s, a través del despliegue de esquemas de certificación en áreas tecnológicas claves.

6. Previsión en desafíos de ciberseguridad emergentes y futuros. Comprender las tendencias y patrones emergentes mediante la prospectiva y escenarios futuros que contribuyen a mitigar los desafíos cibernéticos. Evaluación temprana de desafíos y riesgos derivados de la adopción y adaptación a las emergentes futuras opciones, mientras se colabora con las partes interesadas en estrategias apropiadas de mitigación.

7. Eficiente y efectiva información de Ciberseguridad y conocimiento para su gestión en Europa. Gestión compartida de la información y el conocimiento para el ecosistema de ciberseguridad en UE, a través de un formulario accesible, personalizado, oportuno y aplicable, con metodologías adecuadas, infraestructura, herramientas y metodologías acoplados al aseguramiento de la calidad, para alcanzar servicios de mejora continua. (ENISA, 2020)

Ahora bien, es muy importante resaltar, que el esfuerzo europeo en su lucha contra el cibercrimen y el esfuerzo conjunto para combatirlo como bloque ha dado como resultado el primer tratado internacional sobre ciberdelincuencia. Este tratado es el convenio de Budapest, el cual busca poder enfrentar la cibercriminalidad ante los diferentes

delitos informáticos y demás amenazas y modalidades delictivas que se ejecutan en la web. Violaciones contra derechos de autor, fraude relacionado a la computación, pornografía infantil y violaciones se seguridad de los sistemas son compromisos con los que particularmente se lidia desde esta convención. Del mismo modo, comprende un protocolo suplementario en Xenofobia y racismo cometidos a través de los sistemas de computación.

Este tratado, mediante la transversalización de leyes en los diferentes países, ha logrado propiciar mejores prácticas desde el punto de vista de investigación y cooperación entre los miembros. Liderado por el consejo de Europa y con el apoyo de observación de Canadá, China y Japón, fueron fue aprobado en 2001 y de manera común, siguen trabajando por buscar una política criminal que proteja la sociedad ante el cibercrimen, a través de la adopción de legislaciones apropiadas y fomentando la cooperación internacional. (Treaty Office).

A agosto de 2020, el convenio de Budapest cuenta con 65 miembros, entre los que se encuentran los siguientes países de la región Latinoamericana: Argentina, Chile, Colombia, Costa Rica, Panamá, Paraguay, Perú y República Dominicana. Desde la perspectiva internacional y considerando también a los países que son influencias mundiales, vale la pena mencionar a los siguientes: Canadá, Japón, Australia, Canadá, Estados Unidos, Reino Unido, Suiza, Noruega, Holanda, Israel, Dinamarca, Francia, Alemania, Bélgica.[2]

Pero ¿desde América latina como estamos enfrentando la ciber exposición?, ¿cómo se encuentran los países en materia de ciberseguridad?

Si bien instituciones como la OEA y el BID han venido haciendo esfuerzos por empezar a hablar del tema con un enfoque regional, es claro que aún hace falta camino por recorrer. Los delincuentes, ladrones y criminales mutan velozmente. Además, estos no conocen fronteras y operan de acuerdo con sus necesidades. Hoy esta forma de delincuencia es multisectorial y opera de manera multinacional. Por eso ante dicho enfoque, urgen estrategias, convenios y cooperación con enfoque multilateral y regional que permitan armonizar la labor de las autoridades nacionales.

FELABAN sobre este considera importante que las soluciones cooperativas y de alcance supranacional, tengan un mayor protagonismo hacia el futuro. Sobre el particular y con el debido permiso de sus órganos directivos se viene proponiendo el proyecto FIC. El mismo aborda la dimensión del fraude financiero para generar información y prevención de los problemas que hoy pueden generarse en este frente. Esto resulta de ser de interés de toda la comunidad bancaria y financiera ya que, el mismo es pionero en su género.

Sobre el proyecto del FIC podemos ofrecer información en tendencias del fraude en la región para la industria financiera, recolección de

Países miembros de la convención de Budapest: Albania, Andorra, Armenia, Argentina, Australia, Austria, Azerbaiyán, Bélgica, Bosnia y Herzegovina, Bulgaria, Cabo verde, Canadá, Chile, Colombia, Costa Rica, Croacia, Chipre, República checa, Dinamarca, Republica dominicana, Estonia, Francia, Georgia, Alemania, Ghana, Grecia, Hungría, Islandia, Israel, Italia, Japón, Letonia, Liechtenstein, Lituania, Luxemburgo, Malta, Mauricio, Moldavia, Mónaco, Montenegro, Marruecos, Holanda, Macedonia del norte, Noruega, Panamá, Paraguay, Perú, Filipinas, Polonia, Portugal, Romania, San Marino, Senegal, Serbia, Eslovaquia, Eslovenia, suiza, España, Sri Lanka, Tonga, Turquía, Ucrania, Reino Unido y Estados unidos.

Países observadores: Benín, Brasil, Burkina faso, Guatemala, Irlanda, México, Nigeria, Níger, Rusia (en calidad de miembros de la UE), Sudáfrica, Suecia, Tunicia.

información y análisis de los datos recolectados, que permitan la toma de decisiones en estrategias preventivas, alertas de eventos con relación a puntos de compromiso, puntos de testeo, puntos de materialización y comercios riesgosos; así como intercambio de buenas prácticas y retroalimentación sobre las diferentes herramientas, mecanismos y estrategias de prevención.

Como documento anexo, dejamos un recuento del estado en materia de estrategias nacionales de ciberseguridad en los países latinoamericanos, en el que se puede encontrar que países cuentan con una estrategia, el año de entrada en vigor, los responsables y la descripción de cada una.

Bibliografía recomendada sobre el tema

FELABAN, Cápsula de ciberseguridad, 2020, publicación edición # 1.

The White house, National Cyber Strategy, United States of America, 2018. En: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

ENISA, ENISA's work on National Cybersecurity Strategies, consultado en Agosto 2020, en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies#:~:text=A%20national%20cybersecurity%20strategy%20(NCSS,achieved%20in%20a%20specific%20timeframe.

ENISA, A trusted Cyber secure Europe, Junio de 2020, encontrado en: https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secure-europe-enisa-strategy

Treaty Office, Details of Treaty No. 185, Convention on Cybercrime, consultado en Agosto de 2020, en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Ministerio de Relaciones Exteriores, Colombia se adhiere al convenio de Budapest contra la ciberdelincuencia, marzo de 2020, en: https://id.presidencia.gov.co/Paginas/prensa/2020/Colombia-se-adhiere-al-Convenio-de-Budapest-contra-la-ciberdelincuencia-200317.aspx#:~:text=%E2%80%8B%E2%80%A2%20El%20Convenio%20de,%2C%20Panam%C3%A1%2C%20Paraguay%20y%20Per%C3%BA.&text=El%20Convenio%20entrar%C3%A1%20en%20vigor,17%20de%20marzo%20de%202020.

Council of Europe, Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY, Cybercrime, consultado en Agosto de 2020, en: https://www.coe.int/en/web/cybercrime/parties-observers

SECRETARÍA GENERAL DE FELABAN

GIORGIO TRETTENERO CASTRO
Secretario General
gtrettenero@felaban.com

JORGE ARTURO SAZA G.
Director Económico
jsaza@felaban.com

DANIEL JUVINAO
Director Concentrador de Fraudes Regional y
Proyectos especiales
djuvinao@felaban.com

LAURA M. GORDILLO V.
Directora Adjunta Concentrador de Fraudes Regional
lgordillo@felaban.com

ADRIANA RODRÍGUEZ
Diseñadora Gráfica
arodriguez@felaban.com

FIC FRAUD INFORMATION CONTROL by FELABAN

FELABAN FEDERACION LATINOAMERICANA DE BANCOS
55 AÑOS 1965 - 2020

siganos en:

https://www.felaban.net
https://cfr.felaban.net

Panorama de la estrategia de ciberseguridad en LATAM

PAÍS	¿Cuenta con estrategia) Año en Vigor	¿En qué consiste?
Argentina	SI -2019	(i) concientización del uso seguro del ciberespacio, (ii) capacitación y educación en el uso seguro del ciberespacio, (iii) desarrollo del marco normativo, (iv) fortalecimiento de capacidades de prevención, detección y respuesta, (v) protección y recuperación de los sistemas de información del sector público, (vi) fomento de la industria de la ciberseguridad, (vii) cooperación internacional, y (viii) (viii)) protección de las infraestructuras nacionales de información críticas. https://www.marval.com/publicacion/estrategia-nacional-de-ciberseguridad-de-la-republica-argentina-13372&lang=es#:~:text=Estrategia%20Nacional%20de%20Ciberseguridad%20de%20la%20Rep%C3%BAblica%20Argentina,-19%20de%20junio&text=El%2024%20de%20mayo%20de,Ejecutiva%20del%20Comit%C3%A9%20de%20Ciberseguridad.
Chile	SI -2017	Los objetivos para el año 2022 son seis, cada uno de los cuales contiene una serie de objetivos específicos. **A continuación, se exponen sucintamente los objetivos generales y sus respectivos objetivos específicos.** (i) Desarrollar una infraestructura de las TIC que, bajo una óptica de gestión de riesgos, sea capaz de resistir y recuperarse de incidentes de ciberseguridad. (ii) Garantizar los derechos de los ciudadanos en el ciberespacio. (iii) Desarrollar una cultura de ciberseguridad en torno a la responsabilidad en el uso de las TIC, a las buenas prácticas y a la educación. (iv) Establecer relaciones de cooperación con otros actores en materia de ciberseguridad y participar de forma activa en foros internacionales. (v) Desarrollar una industria de la ciberseguridad chilena, que sea útil a los objetivos estratégicos del país. http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latina

Panorama de la estrategia de ciberseguridad en LATAM

PAÍS	¿Cuenta con estrategia) Año en Vigor	¿En qué consiste?
COLOMBIA	SI -2016	**Para proteger a los ciudadanos de los riesgos informáticos, el gobierno creará tres dependencias:** (i) El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - ColCERT, encargado de coordinar a escala nacional los aspectos de ciberseguridad. (ii) El Comando Conjunto Cibernético de las Fuerzas Militares, que tendrá la responsabilidad de salvaguardar los intereses nacionales en el ciberespacio. (iii) El Centro Cibernético Policial, estará a cargo de la prevención, la investigación y apoyará la judicialización de los delitos informáticos. Para ello, contará con un comando de Atención Inmediata Virtual (CAI Virtual) para recibir las denuncias de los ciudadanos. La Estrategia incluye cuatro principios fundamentales y cinco dimensiones estratégicas que guían la consecución de los objetivos. En este sentido, se establece un objetivo general, cinco objetivos específicos y 18 estrategias que se implementarán para lograrlos. **Los cuatro principios fundamentales por lo que se rige la Estrategia son:** (i) Salvaguardar los derechos humanos y los valores fundamentales, cuya limitación, en el caso de que sea necesaria, ha de hacerse con apego a la Constitución; (ii) Adoptar un enfoque incluyente y colaborativo que, de forma activa, involucre a las partes interesadas; (iii) Asegurar una responsabilidad compartida, promoviendo la cooperación y colaboración entre las partes interesadas; y (iv) Adoptar un enfoque basado en la gestión de riesgos, que permita a los ciudadanos llevar a cabo sus actividades en el entorno digital de manera segura. **Por su parte, las cinco dimensiones estratégicas son;** (i) Gobernanza de la seguridad digital, mediante la articulación de las partes interesadas, bajo el liderazgo del Gobierno de la Nación; (ii) Marco legal y regulatorio de la seguridad digital, que recoja los aspectos necesarios para adoptar la Estrategia; (iii) Gestión sistemática y cíclica del riesgo de seguridad digital, a través de los procedimientos, metodologías e iniciativas necesarias; (iv) Cultura ciudadana para la seguridad digital, mediante la sensibilización de las partes i nteresadas; y (v) fortalecimiento de las capacidades para la gestión del riesgo de seguridad digital de todas las partes interesadas. **Objetivos específicos:** (i) Establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos, involucrando a las partes interesadas (ii) Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de la seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital. (iii) Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos. (iv) Fortalecer la defensa y la soberanía nacional en el entorno digital con un enfoque de gestión de riesgos. (v) Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital, a nivel nacional e internacional. https://www.mintic.gov.co/portal/inicio/1604:CONPES-aprobo-estrategia-de-ciberseguridad-y-ciberdefensa-para-contrarrestar-amenazas-informaticas-en-el-pais#:~:text=Con%20la%20aprobaci%C3%B3n%20del%20Conpes,o%20incidentes%20en%20el%20ciberespacio.http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latina

Panorama de la estrategia de ciberseguridad en LATAM

PAÍS	¿Cuenta con estrategia) Año en Vigor	¿En qué consiste?
Costa Rica	SI -2017	**La Estrategia Nacional de Ciberseguridad costarricense cuenta con cuatro principios rectores:** (i) Las personas son prioridad, por ello se busca promover el uso de las TIC para mejorar su calidad de vida de forma segura; 2) Respeto a los Derechos Humanos y la Privacidad, principio que debe regir todas las acciones y medidas que se deriven de la Estrategia; (ii) Coordinación y corresponsabilidad de múltiples partes interesadas, en el proceso de implementación de las acciones que se deriven de la Estrategia y, cuando sea pertinente, en el diseño de estas; y (iii) Cooperación Internacional, con entidades públicas y privadas. **8 objetivos:** (i) Coordinación Nacional. (ii) Conciencia pública. (iii) Desarrollo de la Capacidad Nacional de Seguridad Cibernética (iv) Fortalecimiento del marco jurídico en Ciberseguridad y TIC. (v) Protección de Infraestructuras Críticas. (vi) Gestión del Riesgo. (vii) Cooperación y Compromiso Internacional. (viii) Implementación, Seguimiento y Evaluación. https://www.telesemana.com/blog/2017/10/12/costa-rica-presento-su-estrategia-nacional-de-ciberseguridad/https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf
Ecuador	En Desarrollo	(i) Fomentar una cultura y desarrollar conocimientos de ciberseguridad en la sociedad. (ii) Crear marcos legales, normativos efectivos y fomentar la cultura de ciberseguridad responsable en la sociedad. (iii) Diseñar políticas, estrategias de seguridad cibernética, crear marcos legales y regulatorios efectivos. (iv) Diseñar políticas, estrategias de seguridad cibernética, fomentar la cultura de ciberseguridad responsable en la sociedad. (v) Crear marcos legales y regulatorios efectivos para controlar los riesgos en infraestructura crítica nacional, a través de estándares, tecnologías y organizaciones. (vi) Crear marcos legales, normativos efectivos, diseñar políticas y estrategias de ciberseguridad. (vii) Desarrollar conocimiento de la ciberseguridad y controlar los riesgos, a través de estándares, organizaciones y tecnologías. (viii) Crear marcos legales, reglamentarios efectivos y mejorar la resiliencia de la ciberseguridad mediante la respuesta a incidentes, la gestión de crisis, la redundancia, la protección de infraestructura crítica. (ix) Diseñar políticas, estrategias de ciberseguridad cibernética y controlar los riesgos, a través de estándares, organizaciones y tecnologías. https://www.gobiernoelectronico.gob.ec/ecuador-culmina-la-primera-fase-para-la-elaboracion-de-la-estrategia-nacional-de-ciberseguridad/#:~:text=Esta%20actividad%20se%20realiz%C3%B3%20en,y%20asegure%20su%20entorno%20digital.&text=Dise%C3%B1ar%20pol%C3%ADticas%2C%20estrategias%20de%20seguridad%20cibern%C3%A9tica%2C%20fomentar%20la%20cultura%20de,ciberseguridad%20responsable%20en%20la%20sociedad.

Panorama de la estrategia de ciberseguridad en LATAM

PAÍS	¿Cuenta con estrategia) Año en Vigor	¿En qué consiste?
El Salvador	NO	Contiene la normativa y lineamientos para la prevención, detección y remediación de posibles vulnerabilidades a las que se puedan exponer los diferentes recursos de información del país, y proteger la infraestructura crítica nacional. Elaborar e implementar una Estrategia Nacional de Ciberseguridad y política de seguridad digital del Estado, para proteger la información digital en poder del Estado a través de la adopción de estándares internacionales y el trabajo articulado de las instituciones públicas. Elaborar registro y plan de gestión de infraestructura crítica del Estado para identificar riesgos y mitigar amenazas a la infraestructura que soporta los servicios prioritarios nacionales. Fortalecer la gestión del dominio de nivel superior (TLD por sus siglas en inglés) asignado a El Salvador (.SV) para garantizar la seguridad de los portales e impulsar el uso de dominios nacionales en nuestro país. Implementar Centros de Operaciones de Seguridad (SOC) sectoriales para responder a las necesidades específicas de las diferentes áreas y servicios que administra el Estado. Implementar programas de capacitación en ciberseguridad para empleados públicos para garantizar las competencias mínimas y asegurar la información en poder del Estado, para prevenir y mitigar los riesgos derivados de los delitos informáticos. Fortalecer la gestión y los alcances de SalCERT de forma que el Estado pueda contar con una gobernanza claramente definida y con lineamientos actualizados de ciberseguridad. https://www.presidencia.gob.sv/ciberseguridad/
Guatemala	Si - 2018	(i) El capítulo (I) Diagnóstico Nacional de la Seguridad Cibernética en Guatemala, presenta la justificación para la elaboración de esta Estrategia por medio de: información relevante del nivel de penetración de internet; evaluación de infraestructuras críticas; índice de desarrollo en las tecnologías de información y telecomunicaciones; investigación y estado de respuesta a incidentes cibernéticos; y la gestión gubernamental relacionada a la seguridad cibernética. (ii) En el capítulo (II) Construcción de la Estrategia, se detalla la metodología utilizada y adaptada de organismos internacionales como la Organización de Estados Americanos y la Unión Europea; así también, de los lineamientos y la orientación técnica que proveyó la Secretaría de Planificación y Programación de la Presidencia (SEGEPLAN), para la construcción del presente documento. (iii) En el capítulo (III) se presenta la Visón y Principios Generales que enmarcan los fundamentos que rigen el diseño, así como la fuente de inspiración para la implementación de la Estrategia Nacional de Seguridad Cibernética. (iv) En el capítulo (IV) se describen los Ejes, Objetivos y Acciones que constituyen los elementos base para la construcción de los planes de acción bajo una visión alineada y un enfoque multisectorial. (v) Por último, en el capítulo (V) Gobernanza de la Seguridad Cibernética, se plantea bajo el enfoque de gestión integrada y dentro del marco del Sistema Nacional de Seguridad, la coordinación de la seguridad cibernética a nivel nacional. https://uip.mingob.gob.gt/wp-content/uploads/2019/03/Estrategia-Nacional-de-Seguridad-Cibern%C3%A9tica.pdf

Panorama de la estrategia de ciberseguridad en LATAM

PAÍS	¿Cuenta con estrategia) Año en Vigor	¿En qué consiste?
México	SI -2017	La Estrategia Nacional de Ciberseguridad plantea cinco objetivos estratégicos: Sociedad y Derechos; Economía e Innovación; Instituciones Públicas; Seguridad Pública y Seguridad Nacional. El objetivo general de la Estrategia Nacional de Ciberseguridad es identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano. **Para cumplir con el objetivo general, se establecen 5 objetivos estratégicos:** (i) Sociedad y derechos. (ii) Economía e innovación. (iii) Instituciones públicas. (iv) Seguridad pública. (v) Seguridad nacional. **Para el desarrollo de la ENCS se consideran tres principios rectores:** (i) Perspectiva de derechos humanos. (ii) Enfoque basado en gestión de riesgos. (iii) Colaboración multidisciplinaria y de múltiples actores. **Para alcanzar los objetivos estratégicos se desarrollarán 8 ejes transversales:** (i) Cultura de ciberseguridad. (ii) Desarrollo de capacidades. (iii) Coordinación y colaboración. (iv) Investigación, desarrollo e innovación TIC. (v) Estándares y criterios técnicos. (vi) Infraestructuras críticas. (vii) Marco jurídico y autorregulación. (viii) Medición y seguimiento https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad

Panorama de la estrategia de ciberseguridad en LATAM

PAÍS	¿Cuenta con estrategia) Año en Vigor	¿En qué consiste?
Panamá	SI -2013	El objetivo del Estado panameño, mediante el desarrollo de la Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas, es el de aunar los esfuerzos de sus ciudadanos, empresas e instituciones públicas para redundar en un incremento de la seguridad cibernética que permita el uso confiable de las tecnologías de la información en todos los ámbitos nacionales, todo esto salvaguardando los derechos y libertades fundamentales de los ciudadanos y un entorno económico regulatorio favorable al crecimiento y desarrollo de las empresas y permitiendo el buen funcionamiento del Estado. (Consejo Nacional para la Innovación Gubernamental, 2013: 3). **Se enmarca en 6 pilares:** (i) Proteger la privacidad y los derechos fundamentales de los ciudadanos en el ciberespacio. (ii) Prevenir y detener las conductas delictivas en el ciberespacio o el uso de éste para cualquier tipo de delitos o actos ilícitos. (iii) Fortalecer la seguridad cibernética de las infraestructuras críticas nacionales. (iv) Fomentar el desarrollo de un tejido empresarial nacional fuerte en seguridad cibernética, como referencia para la región. (v) Desarrollar una cultura de seguridad cibernética a través de la formación, innovación y la adopción de estándares. (vi) Mejorar la seguridad cibernética y capacidad de respuesta ante incidentes de los organismos públicos. http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latinahttps://cert.pa/documentos-de-interes/
Paraguay	SI -2017	En el apartado de principios se explicita que el Plan Nacional se implementará mediante la cooperación y coordinación del sector público con la sociedad civil, el sector privado y la academia. **En total, son seis los principios que han de orientar el diseño y la implementación de las políticas públicas de ciberseguridad:** (i) Proporcionalidad de las medidas aplicadas; C (ii) Coordinación de esfuerzos y uso eficiente de recursos escasos; (iii) Responsabilidad compartida entre todos los miembros de la sociedad; (iv) Desarrollo e innovación para desarrollar una economía digital; (v) Cooperación internacional, necesaria por la propia naturaleza de las amenazas; (vi) Monitoreo y evaluación de las políticas públicas de ciberseguridad. **De igual manera, contempla 7 ejes:** (i) Sensibilización y Cultura. (ii) Investigación, Desarrollo e Innovación. (iii) Protección de Infraestructuras Críticas. (iv) Capacidad de Respuesta ante Incidentes Cibernéticos. (v) Capacidad de Investigación y Persecución de la Ciberdelincuencia. (vi) Administración Pública. (vii) Sistema Nacional de Ciberseguridad. http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latinahttps://www.mitic.gov.py/materiales/publicaciones/plan-nacional-de-ciberseguridad-paraguay

Panorama de la estrategia de ciberseguridad en LATAM

PAÍS	¿Cuenta con estrategia) Año en Vigor	¿En qué consiste?
Perú	En Desarrollo	**Ley de ciberseguridad del Perú:** En febrero de 2019, Perú se adhiere al convenio de Budapest, el primer tratado internacional que busca enfrentarse a los delitos informáticos y crímenes realizados a través de Internet. El congreso ya ha desarrollado la ley de ciberseguridad respectiva, esta ley tiene por finalidad, no solo responder a las exigencias que ha asumido el país, sino expandir la cobertura legal que se tiene sobre el uso de Internet a través de leyes como Ley de Protección de Datos Personales. Por ahora la ley de ciberseguridad Perú se encuentra próximo a debate. **Los siguientes 7 puntos pertenecen a esta ley y presentan las acciones que debería tomar el estado próximas a su aprobación.** (i) Fortalecer al Estado en materia de ciberseguridad. (ii) Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en materia de ciberseguridad dentro de la Administración Pública (iii) Desarrollar un Plan de sensibilización y capacitación a todos los ciudadanos respecto a la Ciberseguridad. (iv) Fortalecer la legislación en materia de ciberseguridad, la cooperación internacional y propiciar la adhesión del Perú a los diferentes organismos internacionales en esta temática. (v) Afianzar la integración y coordinación eficaz, entre las diversas Coordinadoras de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública y el sector privado. (vi) Elaborar un Plan de Acción Nacional en Ciberseguridad (vii) Crear el Comité Nacional de Ciberseguridad. https://revistaenergiaynegocios.com/2019/11/06/4-criterios-para-medir-ciberseguridad-de-un-pais/https://www.optical.pe/nivel-de-seguridad-contra-ciberamenazas-en-el-peru/
República Dominicana	SI -2018	**Los pilares de la estrategia nacional de ciberseguridad 2018- 2021 se desarrollan contemplando 4 pilares estratégicos:** (i) Marco legal y fortalecimiento instituciones (ii) Protección de infraestructura crítica nacional e infraestructura TI del estado (iii) Educación y cultura nacional de ciberseguridad (iv) Alianzas nacionales e internacionales https://indotel.gob.do/media/10605/decreto-230-18.pdfhttps://presidencia.gob.do/noticias/consejo-aprueba-planes-para-implementar-la-estrategia-nacional-de-ciberseguridad

Panorama de la estrategia de ciberseguridad en LATAM

PAÍS	¿Cuenta con estrategia) Año en Vigor	¿En qué consiste?
Uruguay	NO	El marco presenta 68 requisitos que incluyen buenas prácticas sobre gobernanza de la seguridad, gestión de riesgos, control de acceso, seguridad de las operaciones, gestión de incidentes y continuidad del negocio; además de un modelo de madurez con el que las organizaciones podrán definir las líneas de acción para mejorar su ciberseguridad: (i) Marco de Ciberseguridad (ii) Guía de implementación (iii) Lista de verificación (iv) Guía de auditoría. El Marco de ciberseguridad cuenta con diversa documentación de apoyo para ayudar en la implementación de los diversos requisitos, dentro de dicha documentación se encuentran: políticas; metodología de análisis de riesgos; plantillas de acuerdos de no divulgación, plan de acción, planes de recuperación (DRP); entre muchos otros. Anexo I: Políticas Anexo II: Plantillas Anexo III: Guías y buenas prácticas Anexo IV: Gestión de riesgos Anexo V: Plan de acción Anexo VI: Procedimientos https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco- ciberseguridadhttps://archivos.agesic.gub.uy/nextcloud/index.php/s/pFXtSiWT47Kdaaz#pdfviewer

FRAUD INFORMATION CONTROL

FIC

FRAUD
INFORMATION
CONTROL
by FELABAN

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

55 AÑOS
1965 - 2020

Primera Plataforma Regional Colaborativa
y Confidencial del Mundo

FIC Felaban | Ficfelaban | Fraud Information Control | Fraud Information Control