Marco Nacional de Regulación sobre Ciberseguridad. Recomendaciones.

Comité Técnico en materia de despliegue de 5G en México.

Mesa 5. Ciberseguridad

INDEX

I. Antecedentes

En el marco del parlamento abierto organizado por el gobierno federal para dar cabida a las distintas propuestas para la integración de una Marco Nacional de cIberseguridad, la Mesa 5, del Comité Técnico en materia de Despliegue de 5G pone a consideración de los miembros del mencionado Comité, el presente documento titulado Marco Regulatorio sobre Ciberseguridad. Recomendaciones, que pretende exponer las conceptos y características que una Ley Nacional de Ciberseguridad debiera abordar.

Objetivo de la Ley

Se sugiere que el objetivo general y/o especifico de la Ley sea federal o general, considere los siguientes puntos:

- Crear o, en su caso, fortalecer los órganos interinstitucionales necesarios en materia de Tecnologías de la Información, Comunicación y Seguridad de la Información que articule los esfuerzos de las dependencias de la Administración Pública Federal, Entidades Federativas y los órganos autónomos constitucionales, para la protección de la sociedad mexicana y de las infraestructuras críticas de información en el ciberespacio coadyuvando a mejorar la resiliencia.
- Adoptar un modelo de gobernanza delimitadas en el alcance de sus atribuciones considerando los diferentes enfoques de los sectores públicos y privados a los cuales sería aplicado el modelo planteado, con pleno apego a las disposiciones de protección de información y datos personales.
- Fomentar la confianza en el entorno digital para propiciar el desarrollo de una economía basada en las nuevas tecnologías.
- Proteger datos personales y privados de las personas físicas y morales.
- Establecer los mecanismos que reforzarán la cooperación público-privada para un entorno de ciberseguridad adecuado.
- Mejorar los mecanismos que reforzarán la cooperación internacional en ámbitos de ciberseguridad de interés comunes.

En el documento denominado “Guía para la elaboración de una estrategia

nacional de ciberseguridad - Participación estratégica en la ciberseguridad"[1] de la Unión Internacional de Telecomunicaciones (UIT), una de las principales recomendaciones en las etapas iniciales es asegurarse que el objetivo principal incluya "una expresión de la visión, los objetivos de alto nivel, los principios y las prioridades que orientan a un país a la hora de abordar la ciberseguridad". Lo anterior de manera que se pueda considerar a la ciberseguridad de forma global en todo su ecosistema digital a nivel nacional, en vez de considerar solo un sector, incidente y/o situación particular.

Así mismo, consideramos que el planteamiento principal de la Ley además de las medidas, los programas y las iniciativas que han de ponerse en marcha, también deben integrarse los recursos asignados para esos efectos y la forma en que deben utilizarse. De manera paralela, el proceso deberá proponer la identificación de las métricas que se utilizarán para verificar que los resultados deseados y objetivos planteados se logren dentro de los presupuestos y plazos establecidos.

Aunado a lo anterior, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en su estudio "*Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*", destaca lo siguiente: "La responsabilidad de la coordinación suele asignarse a un organismo específico ya existente o nuevo, y también se asigna claramente la responsabilidad de los demás organismos gubernamentales implicados, para facilitar la cooperación, fomentar las sinergias, evitar la duplicación y poner en común las iniciativas."

Lo anterior, derivado de que ninguna entidad/organismo vertical existente o de reciente creación puede pretender tener un conocimiento exhaustivo y una autoridad lo suficientemente amplia para gestionar todas las facetas de la ciberseguridad a nivel nacional, se recomienda considerar un enfoque cooperativo y multi parte en la creación de una legislación de ciberseguridad, donde se incluyan a los representantes de los sectores privados y públicos que pudieran ser importantes en la evaluación de dichas medidas a cubrir dentro de la aplicabilidad de la posible ley resultante.

---

1 **https://www.itu.int/es/publications/ITUD/Pages/publications.aspx?lang=es&media=electronic&parent=D-STR-CYB_GUIDE.01-2018**

La Ley deberá identificar y facultar a las autoridades competentes que se encargarán de su ejecución, así como establecer un mecanismo para identificar e incluir a las entidades gubernamentales responsables de la ejecución de la estrategia. El compromiso, la coordinación y la cooperación inter-gubernamentales son funciones básicas de esas instituciones y son además necesarias para velar por que los mecanismos de gobernanza y los recursos asignados produzcan los resultados previstos en la estrategia.

En ese orden de ideas, es recomendable que las entidades señaladas en el campo de aplicación en el ámbito de sus atribuciones y en coordinación con la autoridad competente en materia de Ciberseguridad, puedan emitir las disposiciones administrativas necesarias de carácter general en esa materia, que satisfagan los requerimientos del sector que encabezan.

En la creación de una autoridad competente se debe diseñar y establecer objetivos específicos, cuantificables, viables, basados en resultados y con plazos concretos en el plan de ejecución de la estrategia para una mejor ejecución de sus obligaciones. Al mismo tiempo, se deben destinar los recursos necesarios para la implementación de las estrategias que permitan el logro de los objetivos señalados.

Campo de aplicación

Se recomiendas tomar en cuenta las siguientes consideraciones:

- Que el campo de aplicación prevea los sectores estratégicos, así como a las infraestructuras críticas y servicios esenciales, para revisar la aplicabilidad y forma de la Ley a desarrollar, con la finalidad de evaluar posibles impactos en los diferentes sectores involucrados en dichas iniciativas.
- Que el campo de aplicación haga una diferencia entre seguridad pública (ciberseguridad) y seguridad nacional (ciber defensa) a efecto de crear un solo apartado que le sea aplicable a la seguridad nacional.
- Establecer que la Ley deberá ser observada, entre otros, por la administración pública federal, Entidades Federativas y los órganos autónomos constitucionales.

Definiciones

Se sugiere que para las definiciones que se establezcan en la Ley, se consideren como referencia fuentes internacionales, siempre teniendo en cuenta que la interpretación y/o aplicación sean conformes a conceptos y definiciones establecidas en la Constitución Política de los Estados Unidos Mexicanos (CPEUM), así como a otras leyes vigentes del marco legal de México. Para esto, se sugiere tomar como referencia la experencia internacional en la materia.

Algunos enlaces electrónicos a recursos que ofrecen algunas referencias que puede ser útiles son:

https://www.iso.org/standard/82875.html

https://www.bsi.bund.de/DE/Service-Navi/Cyber-Glossar/cyber-glossar_node.html

https://www.sans.org/security-resources/glossary-of-terms/

https://www.ncsc.gov.uk/section/advice-guidance/all-topics

https://csrc.nist.gov/glossary

https://www.gob.mx/cms/uploads/attachment/file/661790/Glosario_de_Terminos_SD-_SM_compressed.pdf

https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf

https://www.gob.mx/cms/uploads/attachment/file/735044/Protocolo_Nacional_Homologado_de_Gestion_de_Incidentes_Ciberneticos.pdf

https://www.gob.mx/semar/es/articulos/unidad-de-ciberseguridad-279197

Asimismo, se sugiere incorporar las siguientes definiciones:

- Infraestructuras críticas de información.
- Infraestructuras de información esenciales.

De acuerdo a la OCDE, la mayoría de los países con estrategias y/o legislaciones en materia de ciberseguridad cuentan con una definición sobre "infraestructura crítica", la cual se refiere a “los sistemas y redes de información, cuya interrupción o destrucción tendría un grave impacto en la salud, la seguridad, la protección o el bienestar económico de los ciudadanos, o en el funcionamiento eficaz del gobierno o la economía” (*OECD Recommendation on the Protection of Critical*

Information Infrastructures)[2].

Lo anterior implica que la eventual Ley de Ciberseguridad nacional debe ser coherente con su nivel de riesgo. A tal efecto, se debe realizar un análisis de los puntos fuertes y débiles de la ciberseguridad existente en el país y se debe consultar los materiales y documentos importantes en colaboración con las entidades pertinentes del gobierno, organismos autónomos, el sector privado y la sociedad civil. Se sugiere que la Ley incorpore las siguientes definiciones:

- Infraestructuras críticas de información.
- Infraestructuras de información esenciales.

Marco institucional actual

Guardia Nacional y el Centro Especializado en Respuesta Tecnológica

De acuerdo con la Constitución Política de las Estados Unidos Mexicanos (CPEUM) en su artículo 21, la Guardia Nacional es una institución policial de carácter civil, así como un órgano administrativo desconcentrado de la Secretaría de Seguridad y Protección Ciudadana. Asimismo, de acuerdo con las facultades del Presidente, señaladas artículo 89 de la CPEUM, este puede disponer de la Guardia Nacional en los términos que la ley señale[3.]

Asimismo, la Guardia Nacional cuenta con una Coordinación Operativa Interinstitucional de carácter permanente y está integrada por representantes de las dependencias de la Secretaría de Seguridad y Protección Ciudadana, la Secretaría de Defensa Nacional y la Secretaría de Marina. Al respecto, la Coordinación apoya con la coordinación y colaboración estratégica entre las dependencias de la Administración Pública Federal y la Guardia Nacional.

En el caso de la Unidad de Órganos Especializados por Competencia, esta tiene el objetivo de proponer los lineamientos, mecanismos, técnicas generales de investigación y prevención de delitos, así como de atención a mandamientos

[2] **https://www.oecd.org/sti/40825404.pdf**

[3] Constitución Política de los Estados Unidos Mexicanos, México. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

ministeriales y judiciales, mediante la observancia a lo establecido en la normatividad interna, las disposiciones jurídicas aplicables y el respeto a los derechos humanos. En este sentido, una de sus direcciones adscritas es la Dirección General Científica, la cual busca proponer políticas y procedimientos institucionales en la actuación de los servicios técnico-científicos, mediante la aplicación de estrategias contra la ciberdelincuencia, la investigación criminalística y el desarrollo científico-tecnológico para la implementación de las acciones que apoyen las investigaciones en materia de prevención del delito, así como el esclarecimiento de hechos delictivos competencia de la Guardia Nacional. De esta última se destaca entre sus funciones la de implementar las acciones de vigilancia, identificación, monitoreo y rastreo en la red pública de Internet, con la finalidad de prevenir conductas delictivas.[4]

México cuenta con un Centro Especializado en Respuesta Tecnológica, conocido como Centro Nacional de Respuesta a Incidencias Informáticas (CERT MX), previamente parte de la División Científica de la Policía Federal, pero con la promulgación del reglamento de la Ley de la Guardia Nacional pasó a manos de esta última como parte de la Dirección General Científica. En este sentido, de acuerdo con el artículo 9 de la Ley de la Guardia Nacional, está encargada de realizar acciones de vigilancia, identificación, monitoreo y rastreo en la red pública de Internet sobre sitios web, con el fin de prevenir conductas delictivas.[5]

El CERT-MX tiene la misión de brindar los servicios de apoyo en la respuesta a incidentes cibernéticos que afectan a las instituciones en el país que cuentan con infraestructura crítica de información, que incluye la identificación de amenazas y modus operandi de la ciberdelincuencia para el alertamiento a la ciudadanía, mediante la gestión de incidentes de seguridad informática, fungiendo como el único punto de contacto y coordinación dentro y fuera del territorio nacional y actuando en la investigación forense digital y el análisis técnico policial en apoyo

[4]MANUAL de Organización General de la Guardia Nacional, México. https://dof.gob.mx/nota_detalle.php?codigo=5635311&fecha=16/11/2021

[5] Ley de la Guardia Nacional, Diario Oficial de la Federación, 27 de mayo de 2019, México. https://www.dof.gob.mx/nota_detalle.php?codigo=5561285&fecha=27/05/2019

al Ministerio Público.[6]

El CERT-MX realiza el monitoreo en la red pública de internet a fin de prevenir conductas delictivas, obtiene información de diversas fuentes de agencia nacionales e internacionales y colabora con otros equipos de respuesta que conforman la comunidad global del *Forum for Incident Response and Security Teams* (FIRST)[7].

El objetivo de FIRST es reunir a equipos de respuesta a incidentes y seguridad de todos los países del mundo para garantizar una internet segura para todos por medio de plataformas, medios y herramientas para que los equipos colaboren de manera eficiente. [8]

Dentro del FIRST hay otros 11 equipos de México por parte de la industria y otras instituciones como el CERT de la Universidad Nacional Autónoma de México; Centro de Respuesta ante Incidentes Informáticos (CSIRT, por sus siglas en inglés) de AXTEL; BESTEL *Security Operation Center and Incidents Response Teams;* CERT DSI Totalsec; CERT-AT&T México; CSIRT Ikusi México; CSIRT IQsec; Mnemo-CERT; CERT Silent4Business; CERT Scitum; TIC DEFENSE CERT. De ese modo, sería de relevancia considerar dentro de los estatutos de colaboración de la ley a desarrollar, la importancia de dichos centros especializados establecidos en México, que pudieran apoyar a las iniciativas sectoriales en aras de lograr la implementación de mejores estrategias de ciberseguridad.

Estrategia Digital Nacional

Como antecedente, el 22 de marzo de 2021, como parte del Proceso de Planeación para el Desarrollo de la Estrategia Digital Nacional y de la Política Tecnológica, se plantearon una serie de acciones a desarrollarse por la Coordinación de Estrategia Digital Nacional (CEDN).

Lo anterior fundamentado en el artículo 8 de la Ley Orgánica de la Administración

[6] Gobierno de México. ¿Qué es el CERT-MX?. https://www.gob.mx/gncertmx?tab=%C2%BFQu%C3%A9%20es%20CERT-MX?

[7] El FIRST es una organización enfocada en la respuesta a incidentes. https://www.first.org/.

[8] FIRST. *First Teams*. **https://www.first.org/about/mission**

Pública Federal, en la cual se detalla que “el Ejecutivo Federal contará con las unidades de apoyo técnico y estructura que el presidente determine, de acuerdo con el presupuesto asignado a dicha Oficina”, así como que las unidades podrán estar adscritas de manera directa a la Presidencia o a través de la Oficina referida, y desarrollarán, en otras funciones, las políticas del Gobierno Federal en los temas de informática, tecnologías de la información, comunicación y de gobierno digital, en términos de las disposiciones aplicables.[9]

La CEDN tiene la misión de promover e impulsar que las y los mexicanos gocen y se beneficien del acceso a las tecnologías información y comunicación, así como de los servicios de banda ancha e internet.

En este sentido la CEDN, en materia de seguridad de la información, buscaba realizar evaluaciones de seguridad para detectar amenazas y mejorar la gestión de riesgos; implementar sistemas basados en Software Libre, coordinar entre autoridades los procesos de prevención y atención de incidencias cibernéticas; e implementar un protocolo de seguridad digital, así como la promoción de buenas prácticas de prevención a través del CERT-MX.

Asimismo, el CIDGE, como órgano de coordinación Ejecutiva en materia de Gobierno Digital, es también un mecanismo para la articulación de las políticas tecnológicas de la CEDN, sin embargo de acuerdo con el Proceso de Planeación para el Desarrollo de la Estrategia Digital Nacional y de la Política Tecnológica, posiblemente se modifique, actualice o sustituya el CIDGE a fin de hacerlo armonizable con el marco normativo actual para mejorar la coordinación operativa en la implementación de las políticas tecnológicas.[10]

En septiembre de 2021 se publicó en el Diario Oficial de la Federación el acuerdo por el que se expide la Estrategia Digital Nacional (EDN) 2021-2024, con el propósito de orientar el uso y el desarrollo de las TIC al bienestar social. Además, detalla que es de observancia obligatoria para las dependencias y entidades de la Administración Pública Federal, las cuales deberán actuar conforme a su

[9]Ley Orgánica de la Administración Pública Federal, México.

[10] Gobierno de México (2021). Proceso de Planeación para el Desarrollo de la Estrategia Digital Nacional y de la Política Tecnológica. **https://www.gob.mx/cedn/documentos/proceso-de-planeacion-para-el-desarrollo-de-la-estrategia-digital-nacional-y-de-la-politica-tecnologica.**

misión, visión y ejes, así como apegarse a sus principios, objetivos y líneas de acción.

En este sentido, la EDN aterriza las capacidades gubernamentales bajo 5 principios: austeridad, combate a la corrupción, eficiencia en los procesos digitales, seguridad de la información y soberanía tecnológica. En el caso de la seguridad de la información se integra el objetivo específico de promover una cultura de seguridad de la información que genere certeza y confianza a las personas usuarias de los servicios tecnológicos institucionales y gubernamentales. Al respecto, se plantea una colaboración entre autoridades para mejorar los procesos de prevención y atención de incidencias cibernéticas, así como de buenas prácticas de prevención y reacción a través de la colaboración con el CERT-MX.[11]

Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos

Sustentado en la EDN, el Protocolo tiene el objetivo de fortalecer la Ciberseguridad en las Dependencias Federales, Entidades Federativas, Organismos Constitucionales Autónomos, Academia e Instancias del Sector Privado del país, con la finalidad de alcanzar los niveles de riesgo aceptables en la materia, contribuyendo al mantenimiento del orden constitucional, la preservación de la democracia, el desarrollo económico, social y político del país, así como al bienestar de las mexicanas y los mexicanos.

Al respecto, se ha considerado como metodología de aplicación el Marco de Referencia sobre Ciberseguridad del Instituto Nacional de Estándares y Tecnología de Estados Unidos de América (NIST). Dicho Marco hace referencia a las normas y directrices internacionales existentes, así como a las mejores prácticas de la industria, para promover la protección de las infraestructuras críticas mediante la gestión de riesgos. El NIST representa una colección de normas y mejores prácticas que han demostrado su eficacia para proteger los

[11] Estrategia Digital Nacional 2021-2024, 6 de septiembre de 2021, México. **https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#:~:text=La%20Estrategia%20Digital%20Nacional%20que%20se%20desprende%20del%20Plan%20Nacional,mediante%20su%20incorporaci%C3%B3n%20a%20la**.

sistemas informáticos de las ciber-amenazas, garantizar la confidencialidad de las empresas y proteger la privacidad y las libertades civiles de las personas. En este sentido, el Marco es una metodología cuyo objetivo es reducir y gestionar mejor los riesgos de seguridad cibernética y puede ser usado por las partes interesadas para permitirles identificar y priorizar acciones para reducir el riesgo de seguridad cibernética, así como para alinear los enfoques de políticas, negocios y tecnología para manejar dicho riesgo.[12]

Sobre la coordinación para el Protocolo Nacional de Gestión de Incidentes Cibernéticos, el CERT-MX de la Dirección General Científica de la Guardia Nacional, esta fungirá como la única instancia de coordinación entre las Instituciones de la Administración Pública Federal, Entidades Federativas, Organismos Constitucionales Autónomos, Academia e Instancias del Sector Privado del país involucradas. Asimismo, el Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, detalla que las Instituciones deberán contar con un Marco de Gestión de Seguridad de la Información que procure los máximos niveles de confidencialidad, integridad y disponibilidad de la información generada, recibida, procesada, almacenada y compartida por dichas Instituciones, además de que se recomienda que se establezcan y operen un Equipo de Respuesta a Incidentes de seguridad en TIC en las organizaciones.[13]

Sobre la policía cibernética

El Sistema Nacional de Seguridad Pública (SNSP), es quien sienta las bases de coordinación y distribución de competencias, en materia de seguridad pública, entre la Federación, los Estados y municipios, bajo la directriz del Consejo

[12] Instituto Nacional de Estándares y Tecnología (2018). Marco de Ciberseguridad. **https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018es.pdf**.

[13] ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, 6 de septiembre de 2021, México. .**https://www.dof.gob.mx/nota_detalle.php?codigo=5561285&fecha=27/05/2019.**

Nacional de Seguridad Pública (CNSP).

El CNSP es el órgano superior del SNSP, y es presidido por el presidente de la República, e integrado por los Secretarios de Gobernación, Defensa Nacional, Marina, el Procurador General de la República, los Gobernadores de los Estados, el jefe del Gobierno de la Ciudad de México, el Comisionado Nacional de Seguridad, y el Secretario Ejecutivo del SNSP.[14]

El Programa Nacional de Seguridad Pública 2014-2018 estableció dentro de sus estrategias, la detección y atención oportuna de los delitos cibernéticos y previó, como una de sus líneas de acción, el desarrollo de un Modelo de Policía Cibernética para las entidades federativas. En este sentido, en el país, existen Unidades de Policías Cibernéticas en cada uno de los estados de la República Mexicana, las cuales realizan actividades de prevención, vigilancia, identificación, monitoreo y rastreo en la red pública de Internet, con la finalidad de prevenir cualquier situación constitutiva de un delito que pudiera poner en riesgo la integridad física y patrimonial de los habitantes.

El Centro Nacional de Inteligencia

El Centro Nacional de Inteligencia (CNI) se creó el 30 de noviembre de 2018, en sustitución del Centro de Investigación y Seguridad Nacional (CISEN), pero ahora bajo la supervisión de la Secretaría de Seguridad y Protección Ciudadana (SSCP), y conservando las funciones que se establecen en la Ley de Seguridad Nacional.

De acuerdo con la Ley Orgánica de la Administración Pública Federal el CNI funge como un sistema de investigación e información, que contribuye a preservar la integridad, estabilidad y permanencia del Estado mexicano, así como contribuir, en lo que corresponde al Ejecutivo de la Unión, a dar sustento a la unidad nacional, a preservar la cohesión social y a fortalecer las instituciones de gobierno.

Dentro del artículo 19 de la Ley de Seguridad Nacional se mencionan sus

[14] **https://www.gob.mx/sesnsp/acciones-y-programas/que-es-el-consejo-nacional-de-seguridad-publica-cnsp**.

funciones en las que se incluyen[15]:

1. Operar tareas de inteligencia como parte del sistema de seguridad nacional que contribuyan a preservar la integridad, estabilidad y permanencia del Estado Mexicano, dar sustento a la gobernabilidad y fortalecer el Estado de Derecho;
2. Procesar la información que generen sus operaciones, determinar su tendencia, valor, significado e interpretación específica y formular las conclusiones que se deriven de las evaluaciones correspondientes, con el propósito de salvaguardar la seguridad del país;
3. Preparar estudios de carácter político, económico, social y demás que se relacionen con sus atribuciones, así como aquellos que sean necesarios para alertar sobre los riesgos y amenazas a la Seguridad Nacional;
4. Elaborar los lineamientos generales del plan estratégico y la Agenda Nacional de Riesgos;
5. Proponer medidas de prevención, disuasión, contención y desactivación de riesgos y amenazas que pretendan vulnerar el territorio, la soberanía, las instituciones nacionales, la gobernabilidad democrática y el Estado de Derecho;
6. Establecer cooperación interinstitucional con las diversas dependencias de la Administración Pública Federal, autoridades federales, de las entidades federativas y municipales o delegacionales, en estricto apego a sus respectivos ámbitos de competencia con la finalidad de coadyuvar en la preservación de la integridad, estabilidad y permanencia del Estado Mexicano;
7. Proponer al Consejo el establecimiento de sistemas de cooperación internacional, con el objeto de identificar posibles riesgos y amenazas a la soberanía y seguridad nacionales;

[15] Ley de Seguridad Nacional, México. **https://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac_200521.pdf**.

8. Adquirir, administrar y desarrollar tecnología especializada para la investigación y difusión confiable de las comunicaciones del Gobierno Federal en materia de Seguridad Nacional, así como para la protección de esas comunicaciones y de la información que posea;
9. Operar la tecnología de comunicaciones especializadas, en cumplimiento de las atribuciones que tiene encomendadas o en apoyo de las instancias de gobierno que le solicite el Consejo de Seguridad Nacional;
10. Prestar auxilio técnico a cualquiera de las instancias de gobierno representadas en el Consejo de Seguridad Nacional, conforme a los acuerdos que se adopten en su seno.

También en el Manual de Organización General de la SSCP, en el caso de la Unidad de Información, Infraestructura Informática y Vinculación Tecnológica de la SSPC, esta tiene la función de establecer mecanismos de coordinación funcional con el Centro Nacional de Inteligencia (CNI), con el propósito de determinar el valor, significado e interpretación de la información sistematizada a favor de los trabajos de inteligencia de la Secretaría.[16]

Marco Legal

En México no se cuenta con una ley en materia de ciberseguridad ni con una ley dedicada al delito cibernético, pero el artículo 211 del Código Penal Federal prevé el delito informático. Sin embargo, de acuerdo con el Reporte de Ciberseguridad 2020 del Banco Interamericano de Desarrollo (BID), estas disposiciones son limitadas y dejan varias lagunas, lo que dificulta la lucha contra el cibercrimen.

De acuerdo con el Código Penal Federal, algunos de los delitos tipificados en México, en los cuales se emplean los sistemas informáticos, electrónicos, Internet, computadoras, programas informáticos como medio o como fin se encuentran: la revelación de secretos, el acceso ilícito a sistemas y equipos

[16] Manual de Organización General de la Secretaría de Seguridad y Protección Ciudadana, México. **https://www.dof.gob.mx/nota_detalle.php?codigo=5606770&fecha=04/12/2020#gsc.tab=0**

informáticos, el acoso sexual, el engaño telefónico, la extorsión telefónica, falsificación de títulos, pornografía, suplantación de identidad, entre otros. Otros delitos en cuya comisión se emplean las TIC son el delito de fraude, el robo, el delito equiparado al fraude, entre otros, por lo que sería de suma importancia evaluar un proceso de homologación de términos generales para la tipificación base de lo que se considera un delito cibernético y en consecuencia planificar una iniciativa con los diferentes organismos pertinentes dentro del país para su evaluación y desarrollo, con la finalidad de ser validados y sustentados en la ley de ciberseguridad a desarrollar.

Riesgos, Amenazas y Vulnerabilidades

Como parte de las consideraciones de riesgos, amenazas y vulnerabilidades, se recomienda considerar dentro del glosario de la ley a desarrollar, las amenazas a las cuales pueden ser expuestos los diferentes sectores a los cuales pudiera aplicar la ley de ciberseguridad, con la finalidad de visualizar medidas de prevención y protección, y de este modo evitar estar expuestos a dichas amenazas que pudieran impactar sus procesos críticos. A continuación, se enlista una serie de riesgos, enunciativos más no limitativos, que pudiera servir de referencia en las consideraciones de riesgos, amenazas y vulnerabilidades a considerar en las definiciones. Basado en informes internacionales, en 2021 y continuando en 2022, las principales amenazas identificadas incluyen las siguientes:

Ransomware

Según el informe de ENISA "*Threat Landscape for Ransomware Attacks*" (Informe ENISA), Figura 1, el ransomware se define como un tipo de ataque en el que los actores de las amenazas toman el control de los activos de un objetivo y exigen un rescate a cambio de la devolución de la disponibilidad del activo. El ransomware ha sido una de las principales amenazas durante el período que abarca el informe, con varios incidentes de alto perfil y altamente publicitados.

Malware

Malware, también conocido como código malicioso y lógica maliciosa, es un término general utilizado para describir cualquier software o firmware destinado a realizar un proceso no autorizado que tendrá un impacto adverso en la confidencialidad, integridad o disponibilidad de un sistema. Tradicionalmente, los ejemplos de código malicioso incluyen virus, gusanos, troyanos u otras entidades basadas en código que infectan un host. El spyware y algunas formas de adware también son ejemplos de código malicioso. Durante el período del Informe ENISA, nuevamente se observa un gran número de incidentes relacionados con malware.

Ingeniería Social

La ingeniería social abarca una amplia gama de actividades que intentan explotar un error humano o comportamiento humano con el objetivo de obtener acceso a información o servicios. Utiliza varias formas de manipulación para engañar a las víctimas para que cometan errores o entreguen información confidencial o secreta. En seguridad cibernética, la ingeniería social atrae a los usuarios a abrir documentos, archivos o correos electrónicos, visitar sitios web o conceder a personas no autorizadas acceso a sistemas o servicios. Y aunque estos trucos pueden abusar de la tecnología, siempre dependen de un elemento humano para tener éxito. Esta categoría de amenazas consta principalmente de las siguientes conductas: *phishing, spearphishing, smishing, vishing, business* e-mail comprometido (BEC), fraude, suplantación y falsificación, que se analizan en el capítulo correspondiente.

Amenazas contra los datos

Las amenazas contra los datos tienen como objetivo obtener acceso y divulgación no autorizados, así como manipular datos para interferir con el comportamiento de los sistemas. Estas amenazas son también la base de muchas otras amenazas, que se discuten en el Informe ENISA. Por ejemplo, ransomware, RDoS (Denegación de servicio de ransomware), DDoS (Denegación de servicio distribuida), que tienen como objetivo denegar el acceso a los datos y,

posiblemente, exigir un pago para restaurar este acceso. Técnicamente hablando, las amenazas contra los datos pueden clasificarse principalmente como violación de datos y fuga de datos. La violación de datos es un ataque intencionado por un ciberdelincuente con el objetivo de obtener acceso no autorizado y la liberación de datos sensibles, confidenciales o protegidos. La fuga de datos es un evento que puede provocar la liberación involuntaria de datos sensibles, confidenciales o protegidos debido, por ejemplo, a configuraciones erróneas, vulnerabilidades o errores humanos.

Amenazas contra la disponibilidad: Denegación de servicio

La disponibilidad es el objetivo de una amplia cantidad de amenazas y ataques, entre los que destaca DDoS. El DDoS apunta a la disponibilidad del sistema y los datos y, aunque no es una nueva amenaza, tiene un papel importante en el panorama de amenazas de ciberseguridad. Los ataques ocurren cuando los usuarios de un sistema o servicio no pueden acceder a datos, servicios u otros recursos relevantes. Esto puede lograrse agotando el servicio y sus recursos o sobrecargando los componentes de la infraestructura de red.

Desinformación

Las campañas de desinformación siguen en aumento, impulsadas por el creciente uso de las plataformas de redes sociales y los medios en línea. Las plataformas digitales son hoy en día una de las principales de información para las noticias y los medios de comunicación. Los sitios sociales, las noticias y los medios de comunicación, incluso los motores de búsqueda, son ahora fuentes de información para muchas personas. Debido a la naturaleza de cómo funcionan estos sitios, que es atrayendo gente y generando tráfico a sus sitios, la información que genera más espectadores suele ser la que se promueve, a veces sin ser validada. Diversos motivos subyacen a las diferencias entre información errónea e intencionalmente falsificada. Aquí es donde entran en juego las definiciones de desinformación e información parcial.

Ataques a la cadena de suministro

Un ataque a la cadena de suministro apunta a la relación entre las organizaciones y sus proveedores. En este caso utilizamos la definición en la que se considera que un ataque tiene un componente de la cadena de suministro cuando consiste en una combinación de al menos dos ataques. Para que un ataque se clasifique como un ataque a la cadena de suministro, tanto el proveedor como el cliente deben ser objetivos. SolarWinds fue una de las primeras revelaciones de este tipo de ataque y mostró el impacto potencial de los ataques a la cadena de suministro.

FIGURA 1: PAISAJE DE AMENAZAS DE ENISA 2022 - AMENAZAS PRINCIPALES

Vulnerabilidades:

Una vulnerabilidad de seguridad es una debilidad que un adversario podría aprovechar para comprometer la confidencialidad, la disponibilidad o la integridad de un recurso. En este contexto, una debilidad se refiere a fallos de implementación o implicaciones de seguridad debido a elecciones de diseño. Por ejemplo, ser capaz de sobrepasar los límites de un búfer mientras se escriben

datos en él introduce una vulnerabilidad de desbordamiento de búfer.

Repositorios de vulnerabilidades públicas:

Las vulnerabilidades de día cero son vulnerabilidades que no se han divulgado públicamente y se mantienen privadas. Hay varios repositorios de vulnerabilidades públicos disponibles que permiten a las partes interesadas tener fácil acceso a la información relativa a vulnerabilidades conocidas. Los repositorios de vulnerabilidad más destacados son CVE, NVD y OVAL. CVE ha establecido un sistema de referencia para registrar vulnerabilidades llamado identificador CVE (CVE-ID). Los CVE-ID suelen incluir una breve descripción de la vulnerabilidad de seguridad y, a veces, avisos, medidas de mitigación e informes.[17]

Gestión de vulnerabilidades

La administración de vulnerabilidades identifica, clasifica, evalúa y mitiga vulnerabilidades. Los profesionales de la seguridad informática realizan el proceso de gestión de vulnerabilidades de manera organizada y oportuna mediante la realización de algunas acciones y procedimientos. A continuación, se muestra una referencia sobre estas acciones:

- **Preparación:** Definir el alcance del proceso de gestión de vulnerabilidades.
- **Análisis de vulnerabilidades:** Los escáneres de vulnerabilidades son herramientas automatizadas que analizan un sistema en busca de vulnerabilidades de seguridad conocidas que proporcionan un informe con todas las vulnerabilidades identificadas ordenadas en función de su gravedad. Los escáneres de vulnerabilidad conocidos son Nexpose, Nessus y OpenVAS.
- **Identificación, clasificación y evaluación de las vulnerabilidades:** El analizador de vulnerabilidades proporciona un informe de las vulnerabilidades identificadas.
- **Remediación de acciones:** El propietario del activo determina cuál de las vulnerabilidades se mitigará.
- **Re-escaneo:** Una vez que se completan las acciones de corrección, se realiza un

[17] https://cve.mitre.org/

nuevo análisis para verificar su efectividad.

Sobre los Derechos Humanos

La Ley de ciberseguridad nacional debe observar los derechos humanos y ser coherente con éstos. Esta Ley debe prestar particular atención a la libertad de expresión, la privacidad de las comunicaciones y la protección de la privacidad de los datos personales de conformidad con lo establecido en las leyes.
Se recomienda promover el establecimiento de mecanismos nacionales de observancia (tanto de aplicación como de incentivos). Estos mecanismos deben establecerse para prevenir, combatir y mitigar las acciones dirigidas en contra la confidencialidad, la integridad y la disponibilidad de la información de los sistemas e infraestructuras de TIC.

Igualmente, debe considerar que desde los sectores involucrados se promuevan mecanismos y actividades de capacitación y sensibilización encaminados a educar a la sociedad en todos sus niveles sobre el entorno en materia de Ciberseguridad, teniendo como finalidad contribuir a la seguridad de los usuarios digitales enfatizando la importancia de la prevención como herramienta de mitigación frente a los posibles riesgos asociados al uso de la tecnología e, igualmente, enfocarse hacia los mecanismos y las actividades de capacitación y sensibilización en la materia, a los sectores más vulnerables, como niños, niñas, adolescentes y adultos mayores, entre otros.

II. Infraestructura Crítica

Se sugiere se establezca en la Ley un capítulo relativo a la infraestructura crítica de información, así como a las infraestructuras esenciales, incluyendo su definición, clasificación y respuesta a incidentes, los criterios mínimos de ciberseguridad que se deberán observar y los encargados de estas infraestructuras. Es de suma importancia que dentro de los estatutos de la ley, se involucren a los diferentes organismos y empresas que son consideradas proveedores de servicios de infraestructuras críticas para hacerlos participes de posibles responsabilidades.

a. Auditorias y pruebas de estrés

Se sugiere que las partes interesadas realicen auditorias y pruebas de estrés para identificar y evitar violaciones a la seguridad de las infraestructuras críticas, que pueden realizarse de forma voluntaria u obligatoria.

En particular, Europa y China cuentan con un régimen de inspección y auditoría para garantizar que los proveedores de servicios y de infraestructuras críticas provean las actividades adecuadas de reducción de riesgos y rindan cuentas si se comprueba que no cuentan con procesos con la capacidad necesaria.

Por su parte, Estados Unidos deja a los proveedores de infraestructuras críticas que inviertan voluntariamente para reducir el riesgo cibernético, y ha desarrollado un conjunto de estándares, metodologías, procedimientos y procesos que alinean los enfoques de políticas, negocios y tecnología para abordar los riesgos cibernéticos.[18]. La integración de un Padrón de Proveedores es recomendable.

b. Gestión de Riesgos

Se sugiere que las partes encargadas de proteger la información y las infraestructuras críticas de amenazas, riesgos e incidentes de ciberseguridad empleen la metodología de la gestión de riesgos.

A efecto de lo anterior, las partes en interesadas podrán establecer los siguientes planes en materia de ciberseguridad[19]:

i. Respuesta ante incidentes cibernéticos
ii. Continuidad de negocio
iii. Respaldo de la información
iv. Plan de recuperación ante desastres

Para el logro de sus objetivos, las partes interesadas deberán considerar el Marco de Gestión de Seguridad de la Información para Proteger, Detectar, Responder y Recuperarse de incidentes de ciberseguridad.

El fortalecimiento de la estrategia de la Resiliencia cibernética nacional y protección de las infraestructuras críticas deberá considerar:

[18] OEA (2018) Gestión del riesgo cibernético nacional, White paper series, Edición 2.

[19] **Texto completo | Argentina.gob.ar**

- Las medidas que abordan la gestión de los riesgos operativos de los usuarios y la seguridad de los productos y servicios tecnológicos deben complementarse con esfuerzos para garantizar que se preste mayor atención a aquellas entidades de gobierno y sus funciones que son fundamentales para la resiliencia nacional.
- Las auditorias y evaluaciones periódicas de los riesgos nacionales, las mediciones de las mejoras y la revitalización de los esfuerzos de gestión de riesgos.
- La colaboración con socios internacionales para intercambiar información y mejorar las acciones en la gestión de riesgos.

En esta materia, el gobierno puede centrarse en:

  - Designar y mejorar la protección y la seguridad de las infraestructuras críticas, diseñando e impulsando la aplicación de líneas de acción específicas.
  - Promover la gestión de riesgos en las cadenas de suministro y procesos, a través de políticas que fortalezcan la alineación y la transparencia en las prácticas de seguridad entre los proveedores globales y locales.
  - Invertir en la respuesta a los incidentes, impulsando la obligación de informar sobre los incidentes de ciberseguridad, que dote a los responsables gubernamentales de información oportuna, precisa y aplicable, y facilite el intercambio bidireccional con los responsables del sector privado y público.

c. Requisitos, definición e identificación de infraestructura crítica

Las infraestructuras estratégicas o críticas son todas aquellas que se consideran esenciales para garantizar el normal funcionamiento de los servicios que proporcionan las diferentes administraciones de un país, que pueden incluir aquellas que abarcan ámbitos muy sensibles para el sector privado.

La infraestructura crítica es un activo o sistema que es esencial para proveer funciones económicas y sociales como: salud, agua, alimentación, seguridad, transporte, energía, sistemas informáticos, servicios financieros, entre otros.

Cabe señalar que los requisitos e identificación de la infraestructura crítica puede variar en el tiempo y de acuerdo con las circunstancias. En este sentido, se

recomienda considerar dentro del glosario de la ley a desarrollar una definición genérica de lo que podría considerar infraestructura crítica y que sea la Agencia Nacional de Ciberseguridad quien defina con más precisión lo que se considerará infraestructura crítica.

III. Consideraciones y Recomendaciones para una Ley Nacional de Ciberseguridad

Operación basada en Gestión de Riesgos

Un marco de Ciberseguridad requiere un enfoque basado en una Gestión de Riesgos, que se compone de tres partes: el núcleo del marco, los niveles de implementación del marco y los perfiles del marco.

El núcleo del marco es un conjunto de actividades de ciberseguridad, resultados deseados y referencias aplicables que son comunes en todos los sectores críticos. El núcleo presenta estándares, directrices y prácticas de la industria de una manera que permite la comunicación de las actividades y resultados de ciberseguridad en toda la organización desde el nivel ejecutivo hasta el nivel de implementación y operaciones. El núcleo del marco se basa en cinco funciones concurrentes y continuas: identificar, proteger, detectar, responder y recuperar (IPDRR). Estas funciones proporcionan una visión estratégica de alto nivel del ciclo de vida de la gestión de riesgos de ciberseguridad de una organización.

Los niveles de implementación del Marco proporcionan contexto sobre cómo una organización ve el riesgo de ciberseguridad y los procesos establecidos para gestionar este riesgo. Los niveles de implementación describen el grado en que las prácticas de gestión de riesgos de ciberseguridad de una organización exhiben las características definidas en el Marco. Estos niveles reflejan una progresión de los niveles informales, respuestas reactivas a enfoques que son ágiles e informados sobre el riesgo. Durante el proceso de evaluación del Marco, una organización debe tener en cuenta sus prácticas actuales de gestión de riesgos, entorno de amenazas, requisitos legales y reglamentarios, objetivos de

negocio, misión y limitaciones organizativas.

El Perfil puede caracterizarse como la alineación de normas, directrices y prácticas con el núcleo del marco en un escenario de implementación particular. Los perfiles se pueden utilizar para identificar oportunidades para mejorar la postura de seguridad cibernética comparando el Perfil Actual con un Perfil Objetivo. Los perfiles se pueden utilizar para realizar autoevaluaciones y comunicarse dentro de una organización o entre organizaciones.
Un perfil permite a las organizaciones establecer una hoja de ruta para reducir el riesgo de ciberseguridad, y que esté alineada con los objetivos organizacionales y sectoriales, considere los requisitos legales/regulatorios y las mejores prácticas de la industria, así como refleje las prioridades de la gestión de riesgos. Dada la complejidad de muchas organizaciones, pueden optar por tener múltiples perfiles, alineados con componentes particulares y reconociendo sus necesidades individuales

La gestión del riesgo es el proceso continuo de identificación, evaluación y respuesta al riesgo. Para gestionar el riesgo, las organizaciones deben comprender la probabilidad de que ocurra un evento y los posibles impactos resultantes. Con esta información, las organizaciones pueden determinar el nivel aceptable de riesgo para alcanzar sus objetivos organizacionales y pueden expresar esto como su tolerancia al riesgo.
Con una comprensión de la tolerancia al riesgo, las organizaciones pueden priorizar las actividades de ciberseguridad, lo que permite a las organizaciones tomar decisiones informadas sobre los gastos en este rubro. Las organizaciones pueden optar por manejar el riesgo de diferentes maneras, incluyendo: mitigar el riesgo, transferir el riesgo, evitar el riesgo o aceptar el riesgo, dependiendo del impacto potencial en la prestación de servicios críticos. El Marco utiliza procesos de gestión de riesgos para permitir a las organizaciones informar y priorizar las decisiones relativas a la ciberseguridad. Admite evaluaciones de riesgos recurrentes y validación de impulsores de negocio para ayudar a las organizaciones a seleccionar los estados objetivo para las actividades de ciberseguridad que reflejen los resultados deseados. Por lo tanto, el Marco da a

las organizaciones la capacidad de seleccionar dinámicamente y dirigir la mejora en la gestión de riesgos de ciberseguridad para todos los sectores.

Ejemplos de procesos de gestión de riesgos de ciberseguridad incluyen la Organización Internacional de Normalización (ISO) 31000:20096, ISO/Comisión Electrotécnica Internacional (IEC) 27005:20117.

Basado en estándares y recomendaciones internacionales

Principios rectores.

Neutralidad tecnológica

El principio de neutralidad tecnológica es el pilar fundamental del desarrollo digital y de la industria de la tecnología de la información y las telecomunicaciones en todos los países; este es un principio mundial y universal. Podemos definirla como aquella en la que ninguna tecnología, ningún proveedor o equipo, será favorecida o discriminada, siendo los operadores o usuarios finales libres de elegir el que más se adapte a sus necesidades. Cabe señalar que tanto la industria como la regulación de las telecomunicaciones tienen una larga tradición de respetar este principio, que se ha manifestado en las regulaciones y jurisprudencia relacionadas con esta industria.

En el escenario de la adaptación de la legislación y la normativa en materia de ciberseguridad, hay que considerar que, la regulación no debe dar elección preferente ni descalificar ninguna tecnología, ya que es el mercado y los consumidores el que tienen derecho a tener acceso y a elegir la que mejor se ajuste a sus requisitos.

Responsabilidad compartida

Una protección y promoción adecuadas de la ciberseguridad requiere compartir la responsabilidad entre los distintos actores de la industria, tanto a nivel de suministro como de usuario. Cabe destacar que el ecosistema en esta área es muy amplio y con múltiples actores, quienes, aunque operan individualmente dentro de sus respectivas áreas de acción, deben estar debidamente coordinados

para dar una respuesta conjunta a un incidente. El hecho de compartir esta responsabilidad implica mejorar las condiciones en el momento de un potencial ataque.

La seguridad cibernética es un desafío común al que se enfrenta la sociedad en su conjunto y es responsabilidad común de todas las partes interesadas, incluidos los gobiernos, las organizaciones industriales, las organizaciones generadoras de estándares, las empresas y los proveedores de tecnología. Si la ciberseguridad se enfoca desde una determinada ideología o está relacionada con factores políticos, los desafíos técnicos del ciberespacio difícilmente se podrán enfrentar con éxito.

La GSMA, organización líder en la industria de las telecomunicaciones, integra la experiencia y los conocimientos de múltiples expertos en evaluación de riesgos, incluyendo la identificación, el análisis y la evaluación de riesgos. en diferentes dominios de redes y subsistemas en una base de conocimiento de ciberseguridad, conocida mundialmente como la "*5G Cybersecurity Knowledge Base*", Figura 2. Esta base de conocimiento proporciona una definición del modelo de responsabilidad de cada actor y el modelo jerárquico de ciberseguridad en las últimas tecnologías móviles inalámbricas.[20]

En general, podemos predefinir las siguientes responsabilidades:

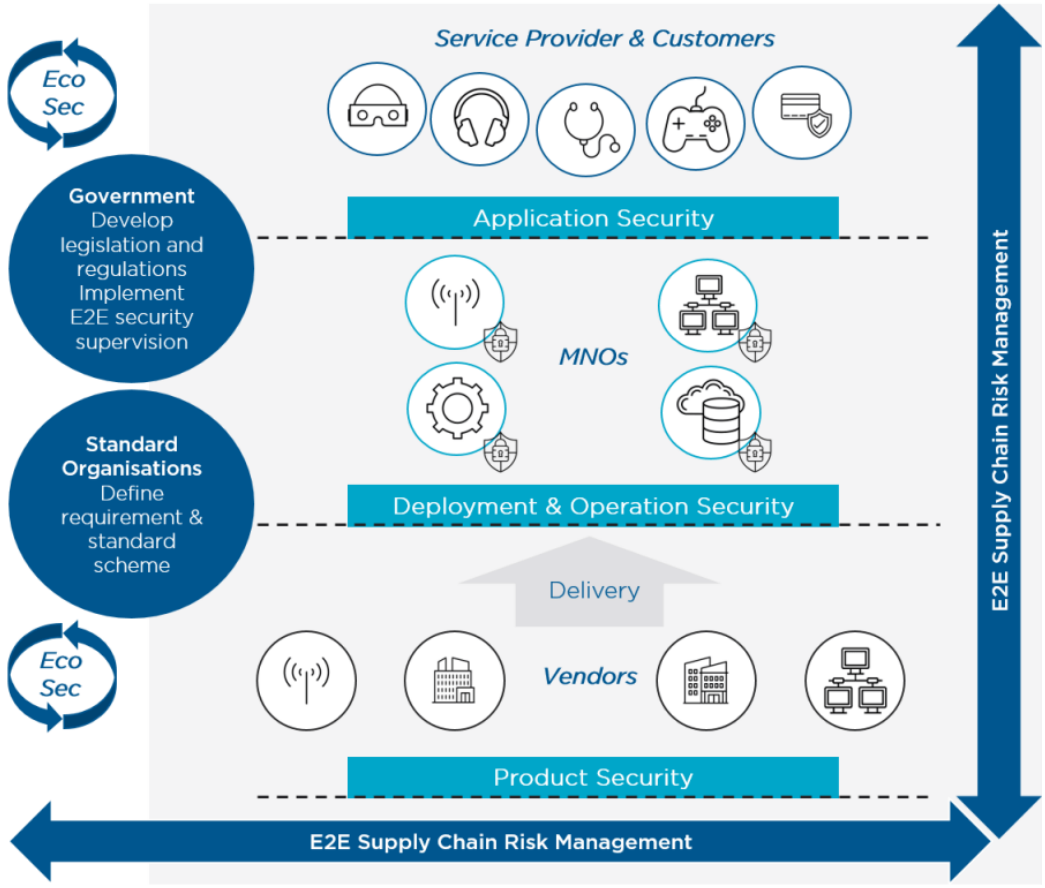
- Los reguladores son responsables de la legislación, la aplicación y la supervisión de la seguridad de extremo a extremo;
- Las organizaciones de normalización definen los requisitos y soluciones del modelo;
- El proveedor del equipo es responsable de la seguridad del producto en la capa identificada como la capa del producto;
- Los operadores son responsables de la implementación de la red y de la seguridad del funcionamiento y mantenimiento respectivos; esto se identifica como la capa de red;
- El proveedor de servicios es responsable de la seguridad de la aplicación; esta

[20] GSMA: (**www.gsma.com**)

se identifica como la capa de aplicación.

Solo cuando todos los actores asuman sus responsabilidades y trabajen estrechamente juntos será viable contar con un ecosistema de ciberseguridad eficaz, abordar conjuntamente sus riesgos y mantener la ciberseguridad de las infraestructuras críticas.

FIGURA 2. MODELO DE RESPONSABILIDAD COMPARTIDA DE LA CIBERSEGURIDAD. FUENTE: BASE DE CONOCIMIENTOS SOBRE SEGURIDAD GSMA 5G.



Colaboración

La ciberseguridad revela una paradoja a resolver, ya que cada empresa o institución tiene la obligación de tomar conciencia sobre los riesgos que supone el uso de las tecnologías en los procesos productivos, en la administración del

negocio particular y en la relación con el cliente. Asimismo, las decisiones estratégicas de cada empresa o institución y la legítima competencia que se produce entre ellas obligan al secreto de sus acciones, por lo que resulta difícil hacer pública cualquier decisión empresarial o cualquier hecho que afecte a sus intereses comerciales y reputación. Sin embargo, la ciberseguridad necesita salir de esta área hermética e incluir el concepto de colaboración como un nuevo eje central de la acción de las empresas, ya que se trata de un problema global y que sin duda afectará, a cada uno de los actores de la sociedad. Por lo tanto, la búsqueda conjunta de soluciones a este problema debe considerar un aspecto colaborativo dentro de la competencia.

Cooperación con la autoridad

Este principio implica que tanto los órganos administrativos públicos como privados deben cooperar con la autoridad competente en la materia para resolver los incidentes de ciberseguridad. Además, si fuera necesario, deberían cooperar también entre los distintos sectores, teniendo en cuenta la interconexión y la interdependencia de los distintos sistemas y servicios.

La realización de este principio es fundamental, ya que responde a la necesidad de comunicar a las autoridades competentes los respectivos incidentes de ciberseguridad y la resolución conjunta de los mismos. Tanto el gobierno como el sector público y privado deben avanzar en la mejora de sus tecnologías, su capital humano y sus defensas contra los ciberataques. Por esta razón, las empresas tienen que ponerse a disposición de la autoridad respectiva, a fin de cooperar con ella y reforzar la cooperación con los demás miembros del sector privado y de la sociedad civil.

Normas y certificaciones internacionales

La realidad de la ciberseguridad y la seguridad de la información requiere la generación de estándares que sean reconocidos por todos y aceptados internacionalmente, ya que esto es lo que genera confianza entre los diversos actores del ecosistema.

Resolver los problemas de seguridad de la red por medios técnicos contribuye a

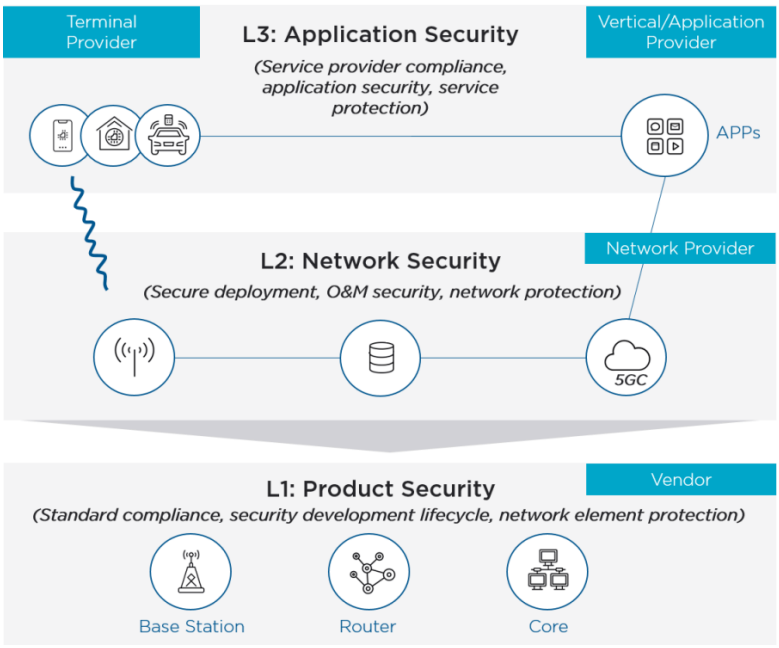
mantener y mejorar la gobernanza de la ciberseguridad, considerando los estándares y mejores prácticas probadas y validadas, (ISO, 3GPP, ITU y GSMA. Estos incluyen la serie ISO 27000, las normas de certificación ISO15408 y la GSMA NESAS).

Cabe señalar que otras regulaciones también pueden desarrollarse con el tiempo, pero deben probarse en varias etapas y madurarse a medida que avanzan las tecnologías y la economía digital. A pesar de ello, lo más importante es que los reglamentos son, por un lado, tecnológicamente neutrales y, por otro, aceptados internacionalmente, además de que no responden a los intereses particulares de los grupos de presión o a las tecnologías específicas.

Certificaciones

Sobre la base de las normas internacionales en relación con los productos o servicios de ciberseguridad, y el nivel recomendado de ciberseguridad del hardware o software informático, los esquemas de certificación recomendados pueden ser necesarios para construir una ciber-resiliencia de extremo a extremo en cada organización e individuo conforme al modelo de seguridad de tres capas mostrado en la Figura 3.

FIGURA 3: CIBERSEGURIDAD, UN MODELO DE SEGURIDAD EN CAPAS



1. ISO/IEC 27001

La ISO/IEC 27001, es el estándar internacional para la gestión de la seguridad de la información. Esta norma fue publicada por primera vez conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) en 2005 y revisada en 2013. En ella se enumeran los requisitos para la arquitectura, la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (ISMS) para ayudar a las organizaciones a que los activos de información que poseen sean más seguros. Este estándar fue actualizado en 2017. Las organizaciones que cumplan con los requisitos que establece pueden solicitar la certificación de una organización calificada después de completar con éxito una auditoría interna. El estándar contiene 11 dominios de control, que incluyen: políticas de seguridad, organización de seguridad de la información, gestión de activos, seguridad de recursos humanos, control de acceso y gestión de operaciones y comunicaciones.

2. ISO 15408

Este estándar propone una serie de funciones de seguridad y requisitos de garantía de seguridad para los productos de TI (que se pueden implementar en hardware, firmware o software) para ayudar a los usuarios a idetificar si satisfacen sus necesidades de seguridad. La norma se centra en la confidencialidad, integridad y disponibilidad, así como en los riesgos causados por factores humanos (maliciosos o no maliciosos) y factores no humanos.

La certificación CC para ISO/IEC 15408 es la certificación de seguridad de productos de TI más reconocida y autorizada en todo el mundo. Actualmente, un total de 30 países se han adherido al acuerdo de certificación mutua CCRA. Esta certificación se evalúa en términos de gestión de la configuración, envío y operación, desarrollo, documentación, soporte de por vida, pruebas y análisis de vulnerabilidades. Hay 7 niveles, y cuanto más alto sea el nivel, más estricta será la evaluación, lo que da como resultado una mayor seguridad.

3. GSMA NESAS

Con el fin de alcanzar un consenso entre los agentes pertinentes sobre la seguridad de los equipos de redes de telecomunicaciones y promover un desarrollo saludable en la fabricación de redes de telecomunicaciones y su

respectiva seguridad operacional, la GSMA ha compilado un conjunto de documentos de orientación denominado *Network Equipment Security Assurance Scheme* (NESAS). El NESAS tiene como objetivo proporcionar una referencia técnica para los proveedores y operadores de dispositivos mediante el desarrollo de líneas de referencia de seguridad reconocidas por la industria. Para los proveedores de equipos, NESAS ayuda a reducir la fragmentación de los requisitos de seguridad debido a las diferencias en los requisitos reglamentarios entre países y regiones, así como los impuestos por el operador. A su vez, para los operadores, NESAS proporciona un método viable para medir si sus proveedores han implementado condiciones de seguridad.

El marco NESAS incluye dos métodos: evaluación de auditoría y evaluación de pruebas. Para la primera, NESAS ha desarrollado una serie de documentos propios para cumplir con el objetivo de la auditoría. Para la evaluación de ensayos, NESAS utiliza las condiciones de la Especificación de Garantía de Seguridad (SCAS) definida por el 3GPP como los requisitos para cumplir los objetivos de dicha evaluación.

4. Base de Conocimientos de Ciberseguridad GSMA 5G

Con la introducción y el lanzamiento de los sistemas 5G por parte de los operadores globales de redes móviles, las redes de comunicación se enfrentarán a nuevas amenazas y desafíos de seguridad. Por lo tanto, se ha vuelto fundamental comprender, mapear y mitigar estas amenazas de seguridad existentes y futuras de manera objetiva.

Para ayudar a los operadores y actores del ecosistema 5G, la GSMA llevó a cabo un análisis integral de amenazas, recopilando información de fuentes públicas como 3GPP, ENISA y NIST por expertos de la industria, incluidos operadores, fabricantes, proveedores de servicios y reguladores. La GSMA ha compilado este análisis en un trabajo llamado "*5G Cybersecurity Knowledge Base*", con el fin de proporcionar una orientación eficaz, con una gama de riesgos de seguridad 5G y medidas de mitigación. Este trabajo fue diseñado para proporcionar a los miembros y partes interesadas de la GSMA un conocimiento integral del ecosistema 5G, con el fin de aumentar la confianza en esa red. Con el tiempo, este trabajo seguirá creciendo y expandiéndose para abordar el panorama cambiante de las amenazas a la ciberseguridad.

Experiencia comparativa, mediciones internacionales.

Entre los indicadores del nivel de ciberseguridad desarrollados alrededor del mundo, se pueden identificar las siguientes: i) el Índice Global de Ciberseguridad (GCI) elaborado por la UIT y ii) el Modelo de Madurez de Ciberseguridad de las Naciones (CMM). Universidad de Oxford.[21][22]

El Índice Global de Ciberseguridad (GCI)

El índice desarrollado por la Unión Internacional de Telecomunicaciones (UIT) mide la mejora y fortalecimiento de la ciberseguridad con valores que oscilan entre 0 y 100 puntos. Contiene cinco pilares: i) Medidas jurídicas; ii) Medidas técnicas; iii) Medidas organizativas; iv) Medidas de fomento de la capacidad; y v) Medidas de cooperación.

Modelo de madurez de la capacidad de ciberseguridad (CCMM)

Se trata de un índice multidimensional que trata de medir la capacidad nacional para ser eficaz en la entrega de seguridad cibernética al país. Contiene las siguientes cinco dimensiones: 1) Política y estrategia de ciberseguridad; 2) Cultura de ciberseguridad responsable en la sociedad; 3) Habilidades y conocimientos de ciberseguridad; 4) Marcos regulatorios y legales efectivos, y 5) Control de riesgos a través de estándares, organizaciones y tecnologías.

El CCMM tiene como objetivo proporcionar una evaluación del nivel de madurez de las capacidades de ciberseguridad de un país, asignando una etapa específica correspondiente a su grado de logro en un área determinada. La evaluación de esta etapa de madurez se clasifica de acuerdo con su nivel de desarrollo: inicial, formativa, consolidada, estratégica y dinámica.[23]

[21] **https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E**

[22] **https://gcscc.ox.ac.uk/the-cmm**

[23] **https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf**

Marco Legal (tipificación de los delitos Unidades Especializadas, mejores prácticas internacionales.)

Legislación integral y federal:

El marco regulatorio, desde la legislación hasta las normas reglamentarias, debe contemplar lo siguiente:

- Tener un objeto bien determinado, toda vez que usualmente se confunde la ciberseguridad en sentido estricto, con el combate a ilícitos que pueden ser cometidos por terceros a través de redes públicas de telecomunicaciones o plataformas de proveedores de servicio de Internet u otros intermediarios, y que no necesariamente implican un riesgo de ciberseguridad.
- Estar alineado estratégicamente con el crecimiento y desarrollo de la digitalización global sin limitar ni sobre-regular el avance del conocimiento, la tecnología, la digitalización y el avance y desarrollo en general.
- Para desarrollar una ley en materia de ciberseguridad es necesario distinguirla claramente en sentido estricto, con el combate a ilícitos que pueden ser cometidos a través de redes públicas y/o privadas, y que no necesariamente implican un riesgo de ciberseguridad. Es importante señalar que la ciberseguridad se refiere primordialmente a la seguridad de la información, es decir, a la protección de los datos contenidos en un sistema informático.
- Debe incluir una delimitación clara de las funciones, responsabilidades interinstitucionales de apoyo y de coordinación entre los tres órdenes de gobierno.
- Debe promover la implementación de políticas de ciberseguridad entre los propietarios, concesionarios y operadores de infraestructuras de información, las cuales consideren medidas y acciones predictivas y preventivas a seguir para garantizar la protección de la información, sistemas, comunicación y almacenamiento en el caso de sufrir ataques cibernéticos.

- Considere las necesidades del mercado para la adopción de servicios de nube y brinde la flexibilidad necesaria para su utilización con la finalidad de generar un entorno más competitivo, a través del libre flujo transfronterizo de datos, de conformidad con los tratados internacionales de los que México es parte, de manera particular el Tratado entre México, Estados Unidos y Canadá.
- El marco regulatorio debe proveer de definiciones y conceptos claros y precisos, que no se presten a confusión o consecuencias negativas no anticipadas.
- No se debe criminalizar el medio comisivo en lugar de la conducta delictiva. En la mayoría de los casos, las conductas delictivas que se cometen por medios electrónicos son las mismas que se cometen en el mundo físico, incluso muchas de ellas ya se encuentran tipificadas en los códigos penales o leyes federales, lo que puede conducir a que se dupliquen los tipos penales. Lo que se debe sancionar es la conducta humana y no el medio a través del cual se comete, es decir, no se debe criminalizar la tecnología, ni a las redes públicas de telecomunicaciones o a las plataformas de proveedores de servicio de Internet u otros intermediarios.
- En la definición de tipos penales se debe garantizar que los intermediarios, infraestructura y repositorios, esto es, las empresas que brindan servicios de acceso a Internet), no deben ser considerados responsables por la actividad ilícita, operación incorrecta o irregular de los usuarios (terceros).
- En la medida en que los delitos informáticos se cometen a través de vías generales de comunicación, deben ser competencia de las autoridades y tribunales federales.

Proteger la privacidad y los datos personales:

- La legislación y la práctica nacionales en materia de ciberseguridad deben estar en consonancia con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Notificación e indagación de incidentes de seguridad:

- Definir la obligación por parte de las instancias de gobierno, de notificar e indagar todos los incidentes de ciberseguridad.
- Divulgar información de violaciones a la ciberseguridad para ayudar a las agencias investigadoras en sus esfuerzos por rastrear incidentes e investigar posibles hechos ilícitos.
- Desarrollar pautas mediante las cuales las entidades privadas pueden evaluar el impacto de una violación y legítimamente sacar conclusiones en cuanto a si ha ocurrido un evento significativo que requiere notificación de conformidad con la legislación en materia de protección de datos personales en posesión de particulares.

Cibercrimen; derecho sustantivo y procesal:

- Marco de justicia penal.
- La investigación de los delitos cibernéticos y el enjuiciamiento de los ciberdelincuentes debe estar respaldada por un sólido marco de justicia penal.
- En caso de que se pretenda abordar la legislación en materia penal, se debe realizar previamente un análisis de los delitos netamente informáticos de aquéllos en los que el uso de Internet, redes de telecomunicaciones y demás TIC son únicamente utilizados como un medio comisivo. Actualmente, el Código Penal Federal ya establece en el Título Noveno (Revelación de secretos y acceso ilícito a sistemas y equipos de informática), un catálogo de delitos informáticos que son adecuados y deben servir como base (artículos 211 Bis 1 al 211 Bis 7).
- México debería llevar a cabo un análisis de su legislación en materia penal, para asegurar que provean a las autoridades encargadas de la investigación y persecución de los delitos cibernéticos (incluyendo policía y fiscales) las herramientas apropiadas que necesitan para el desarrollo de sus funciones.

Consideraciones de procedimiento:

- México debe examinar su derecho procesal y, si es necesario, modificarlo para garantizar la investigación, persecución y sanción de los ciberdelitos.

Estandarizar las actuaciones de los servidores públicos de procuración de justicia en el país en las mejores prácticas para el adecuado manejo de los indicios o materiales probatorios digitales:

- Es posible que deban celebrarse tratados y acuerdos internacionales para establecer mecanismos que permitan la investigación y persecución de los delitos que se cometan en el extranjero y tengan efectos en territorio nacional y viceversa.
- El derecho procesal debe proporcionar los elementos para asegurar y garantizar la cadena de custodia de pruebas y evidencias digitales.
- La volatilidad de los datos electrónicos es un tema altamente sensible.
- Como resultado, la rapidez y la secrecía son vitales para el éxito de una investigación adecuada.
- Resulta necesario promover el intercambio de información y experiencias entre naciones, compañías, organismos y organizaciones en temas de ciberseguridad con el fin de generar conocimientos compartidos que permitan actuar de manera rápida y eficaz ante las ciberamenazas que se presenten y las experiencias obtenidas, sin vulnerar los derechos a la privacidad, así como la información comercial sensible.

Estructura judicial:

- La persecución de los delitos cibernéticos requiere la capacitación de las policías y fiscales para que desarrollen habilidades específicas, recursos y técnicas de investigación para una acción legítima y efectiva en tribunales.
- Designar un departamento central de aplicación de la cibercriminalidad, para reunir la experiencia especializada de la policía y la fiscalía en un solo lugar para una persecución eficiente.
- Una estructura única de punto de contacto resolvería la cuestión de la sub-notificación, debido a la falta de conciencia sobre a quién contactar cuando se detecta un posible delito cibernético.

Implementación del Marco de Ciberseguridad

La implementación de una estructura organizacional que permita la implementación y vigilancia de una Ley Nacional de Ciberseguridad deberá considerar los siguientes aspectos:

- Establecer algunos principios rectores, como la responsabilidad, la integridad de los sistemas, la confidencialidad de los sistemas de información, la disponibilidad de los sistemas de información y el control de daños, entre otros;
- La ley se aplicará a todos los sectores públicos gubernamentales relacionados con la infraestructura de información que debería clasificarse como críticos.
- Las personas con infraestructura de información crítica deben aplicar permanentemente las medidas de seguridad tecnológica, organizativa, física y de la información necesarias para prevenir, informar y resolver incidentes de ciberseguridad y gestionar riesgos, así como contener y mitigar el impacto en la continuidad operativa, la confidencialidad e integridad del servicio prestado. de acuerdo con las disposiciones de la ley.
- Se puede considerar la siguiente estructura de los CSIRT: (i) uno nacional; (ii) uno para el sector público; (iii) uno para el sector de la Defensa Nacional; (iv) potencialmente, cada regulador o regulador sectorial puede establecer su propio CSIRT.
- Se puede crear un Registro Nacional de Incidentes de Ciberseguridad
- Se crea la Comisión Intersecretarial de Ciberseguridad

Se sugiere simplificar la participación de las instituciones, ya que se han establecido una serie de instituciones y organismos que podrían hacer que la Agencia y la gobernanza en su conjunto sean demasiado difíciles en su ejecución. Una estructura institucional poco funcional podría dar lugar a la superposición de funciones o conflictos entre los diferentes órganos creados.

Además de lo anterior, la Agencia debe ser un cuerpo ligero, flexible en su estructura y eminentemente técnico.

Además, el Organismo debería desempeñar un papel de guía y ordenación de las normas administrativas, a fin de evitar la existencia de normas potencialmente contradictorias emitidas por diversos servicios gubernamentales.

Aspectos esenciales y comunes de la estrategia, la legislación y la regulación de la ciberseguridad

A partir de un análisis de la legislación actual y comparativa en materia de ciberseguridad, se identifican cinco puntos comunes:

a) La protección de la infraestructura de información crítica es un enfoque legislativo;
b) Dar importancia a la investigación en ciberseguridad, la innovación tecnológica, la sensibilización y el cultivo del talento;
c) Establecer mecanismos para la vigilancia de la seguridad cibernética, la alerta temprana y el intercambio de información, fortaleciendo los intercambios y la cooperación internacionales;
d) Los administradores de infraestructuras críticas deben adoptar medidas de gestión de riesgos adecuadas y proporcionadas;
e) Las obligaciones de notificación de los incidentes de ciberseguridad son amplias.

Creación de una Agencia Nacional de Ciberseguridad u organismo relacionado

Se puede establecer una Agencia Nacional de Ciberseguridad (Agencia) para asesorar en materia de ciberseguridad, coordinar las acciones de las instituciones relacionadas con este tema y regular y supervisar la estrategia nacional de ciberseguridad. La agencia será funcionalmente descentralizada, y estará relacionada con el Gobierno Federal.

Se puede considerar que la integración de los miembros de esta Agencia incluye la Administración Pública Federal, con el propósito de que una Estrategia

Nacional de Ciberseguridad pueda tener un desarrollo integral, holístico y transversal desde el Gobierno y permita el vínculo con diferentes actores, es decir: sociedad civil, sector privado, las instituciones técnicas y académicas y públicas de nivel federal, estatal y municipal y otras autoridades, incluyendo cualquier institución pública con autonomía.

La Agencia puede tener en cuenta ciertas funciones y responsabilidades con respecto a la Estrategia Nacional de Ciberseguridad:

- Aprobar y difundir normatividad y lineamientos en la materia.
- Hacer un seguimiento y coordinar la aplicación de la Ley en colaboración con los diferentes interesados y entidades gubernamentales;
- Promover la colaboración interinstitucional y los planes de cooperación en materia de ciberseguridad;
- Fomentar la colaboración y la cooperación con las diferentes partes interesadas: sociedad civil, sector privado, comunidades técnicas y académicas

Determinadas funciones y responsabilidades pueden ser consideradas por la Agencia con respecto a la aplicación de la Estrategia de Ciberseguridad, como integrar grupos de trabajo para el desarrollo de cada uno de los vínculos transversales, que impactarán directamente en los diferentes objetivos estratégicos.
Los grupos de trabajo permitirán integrar los esfuerzos, acciones y propuestas de los diferentes actores, de acuerdo con las capacidades y atribuciones de cada una de las partes.

IV. Resiliencia y prevención

Las amenazas, recientemente, han incluido ciberataques contra las infraestructuras digitales nacionales. En algunos escenarios hay infraestructuras tecnológicas con problemas de obsolescencia, lenta modernización y adquisición de tecnología y marcos legales y regulatorios anticuados, lo que aumenta los riesgos para la explotación de vulnerabilidades. Hay desafíos relacionados con el presupuesto disponible y la escasez de personal especializado en ciberseguridad en las

organizaciones, y es necesarop construir sistemáticamente una cultura de ciberseguridad para que las personas y las empresas sepan cómo protegerse en línea.

La Ley Nacional de Ciberseguridad debe considerar las siguientes iniciativas para llevar a los sectores público y privado a un nuevo nivel en ciberseguridad y resiliencia cibernética:

- Fortalecer los aspectos institucionales, regulatorios, administrativos y de gestión para abordar los problemas de ciberseguridad de la alta dirección, creando conciencia y capacitando a todas las partes interesadas;
- Aumentar la confianza digital y fomentar el uso del entorno digital nacional, fortalecer la seguridad de la información, adoptar medidas para gestionar los riesgos de ciberseguridad frente a los activos y desarrollar una cooperación eficiente en la que participen múltiples partes interesadas;
- Proteger los derechos digitales y otros derechos de los ciudadanos y sus actividades económicas y sociales en el entorno digital reforzando la lucha contra la ciberdelincuencia y aplicando mecanismos de asistencia a las víctimas de estos ataques;
- Colaborar activamente y mejorar la comunicación con las organizaciones internacionales en la promoción de mejores prácticas para la resiliencia.
- La resiliencia cibernética requiere establecer componentes de ciberseguridad como la gobernanza, la educación, la cooperación, la regulación, la investigación, la innovación, la diplomacia, el desarrollo, la protección, y a lo público y lo privado, para que el país pueda tener una estructura social y económica que facilite el logro de la resiliencia colaborativa.

a. Respuesta a incidentes

Las partes interesadas deberán observar el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.

El CERT deberá implementar una Plataforma o Sistema electrónico que permitan la gestión, manejo, procesamiento, almacenamiento y/o transmisión de incidentes en materia de ciberseguridad, entre los diferentes centros de respuestas a incidentes a nivel nacional e internacional. El CERT deberá implementar un Área Responsable disponible las veinticuatro horas del día, los trescientos sesenta y cinco días del año para atender la gestión, recepción y/o transmisión de los incidentes en materia de ciberseguridad.

Las partes interesadas deberán establecer y operar un Equipo de Respuesta a Incidentes de Seguridad en TIC en su organización, conforme al Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.

El CERT establecerá política para la divulgación de vulnerabilidades, la cual debe señalar pautas mínimas de atención, criterios de seguridad, y exigir la notificación de incidentes cibernéticos a las partes.

Respuesta a incidentes:

- El gobierno debe revisar las capacidades actuales de respuesta de sus diversas dependencias, entidades y organizaciones y considerar la necesidad de que cada una mantenga y realice periódicamente procedimientos formalizados de respuesta a incidentes.
- Todos los incidentes del sector público deben ser reportados, sirviendo como el punto central de información para todos los incidentes federales de seguridad de la información, de acuerdo con las directrices especificadas para la presentación de informes.
- Los incidentes que tienen el potencial de perjudicar la infraestructura critica nacional, la seguridad nacional, el impacto en la economía y la salud y seguridad pública, entre otros, requieren de sus propios procedimientos especiales que reconocen la ciberseguridad como una responsabilidad compartida e involucrando a todos los niveles de gobierno.
- Dividir la respuesta de incidentes en tres roles y designar un centro principal para cada una de estas áreas de respuesta y situar el liderazgo dentro de la agencia

nacional de ciberseguridad o el ente similar propuesto:

- Identificar, perseguir e interrumpir a los autores de violaciones y sus actividades (respuesta a la amenaza).
- Apoyo de inteligencia para todas actividades.
- Apoyo de análisis forense.

b. Gestión de Crisis

• Para planear la gestión de crisis y mitigación de riesgos, el gobierno debería participar en ejercicios de capacitación y simulaciones que cubran múltiples escenarios, utilizando los resultados para revisar y analizar las políticas y procedimientos e informar sobre la toma de decisiones estratégicas.

c. Información actualizada

• Se recomienda desarrollar una estrategia integral para el intercambio de información y la colaboración que pueda ayudar a identificar las prioridades, establecer valores compartidos y fijar el rumbo para construir procesos eficaces de intercambio de información.

• Para generar confianza, sobre todo en las fases iniciales del intercambio de información, se deben compartir información procesable, mejores prácticas y procedimientos globalmente aceptados para que los operadores puedan defender mejor las redes.

• Es necesario promover esquemas de colaboración e intercambio de información entre los sectores privado y público. Cuando existan requerimientos de entrega de información por seguridad nacional/pública, además de un fundamento legal, un alcance limitado, estar armonizados en todos los sectores y ser racionalizados para evitar la duplicación de esfuerzos y las obligaciones de cumplimiento contraproducentes.

• Los programas de intercambio de información deben ser voluntarios.

• La coordinación y el intercambio de información debe ser un proceso bidireccional.

• El intercambio de mejores prácticas es un ámbito en el que el gobierno puede

desempeñar un papel proactivo comprometiéndose con otros actores.

• Fomentar el intercambio global de las mejores prácticas.

• El gobierno debe hacer uso de sistemas y procesos redundantes de respaldo que estén aislados o segmentados de los sistemas principales, pero fácilmente disponibles para su uso para evitar interrupciones.

• Los planes de recuperación, incluida la medida de respaldo/redundancia digital vigente, deben ser ejercidos, reevaluados y actualizados periódicamente.

Informes y reportes periódicos

- Mantener y fortalecer los esfuerzos de iniciativas para incidir en la percepción que tienen de la ciberseguridad los encargados de la seguridad informática de las organizaciones.
- Fortalecer la actual estrategia nacional de ciberseguridad basada en un marco jurídico que contemple informes y reportes periódicos que estén a disposición de las partes interesadas en temas de la predicción, prevención, investigación, sanción, mitigación y concientización, así como aspectos jurídicos que fortalezca el Estado de Derecho, como un pilar central en el contexto de desarrollo económico, la transformación digital, la innovación y el bienestar social.
- Enfatizar las ventajas de mitigar riesgos como una actividad permanente en el negocio y en la planeación y evaluación de resultados.
- La evaluación de la ciberseguridad en la industria de tecnologías de la información y comunicaciones es fundamental. Muchas organizaciones de integración, desarrollo de software y consultoría, al ser proveedores de los departamentos de sistemas y control de procesos, pueden implementar valoraciones y tener conciencia de la madurez de su seguridad en apego a las mejores prácticas en ciberseguridad.
- Es necesario que exista un organismo de coordinación que integre la información relevante de todos los actores responsables para prevenir, investigar, accionar, sancionar y concientizar y, para llevar a cabo esta importante tarea necesariamente debe participar el sector privado, gobierno, academia y sociedad civil.
- Crear un observatorio de los ataques cibernéticos en otros países para, en su caso, adoptar medidas de prevención.

Cooperación nacional e internacional

- La cooperación internacional y entre los sectores público y privado en materia de prevención y respuesta a la ciberdelincuencia es especialmente crítica debido a su naturaleza.
- Los ciberdelincuentes operan más allá de las fronteras nacionales, a través de grupos delictivos organizados a nivel mundial y de personas vinculadas a la cadena de suministro de la ciberdelincuencia situadas en todo el mundo, y se dirigen a víctimas de diversas jurisdicciones.
- Se necesitan respuestas políticas y operativas eficaces para combatir la ciberdelincuencia y permitir una cooperación internacional y público-privada efectiva.
- Para reforzar la cooperación en materia de enjuiciamiento y otras acciones legales para combatir, desintegrar y disuadir la ciberdelincuencia, es fundamental que el gobierno adopte leyes coherentes a nivel mundial, que incluyan disposiciones sustantivas y procesales sobre los delitos y las investigaciones.
- El gobierno y las organizaciones del sector privado también pueden reforzar la cooperación en las actividades de predicción prevención y respuesta.
- El gobierno debe explorar la creación de una estrategia para una coordinación y cooperación eficaces con los organismos internacionales de aplicación de la ley y los aliados en ciber inteligencia.
- Esta estrategia puede incluir la coordinación con otros organismos nacionales para facilitar el análisis, la investigación y persecución de hechos delictivos así como el intercambio de información sobre amenazas.

Se reitera que debe observarse el Tratado entre México, Estados Unidos y Canadá (T-MEC) y también el Tratado Integral y Progresista de Asociación Transpacífico (TIPAT), en materia de comercio digital:

Ambos tratados incluyen un capítulo de Comercio Digital que tiene como objetivo promover la prosperidad económica, un comercio más justo y la competitividad. Dicho capítulo contiene diversos artículos relativos a ciberseguridad, que deben ser observados sin excepción en el marco jurídico y propuestas legislativas en

esa materia -y que han sido recogidos también en otros tratados y acuerdos comerciales internacionales-:

- Ciberseguridad (Art. 19.15 del T-MEC y 14.16 del TIPAT).
- Protección de la Información Personal (Art. 19.8 del T-MEC y 14.8 del TIPAT).
- Transferencia Transfronteriza de Información por Medios Electrónicos (Art. 19.11 del T-MEC y 14.11 del TIPAT).
- Ubicación de las Instalaciones Informáticas (Art. 19.12 del T-MEC y 14.13 del TIPAT).
- Comunicaciones Electrónicas Comerciales No Solicitadas (Art. 19.13 del T-MEC y 14.14 del TIPAT).
- Código fuente (Art. 19.16 del T-MEC Y 14.17 del TIPAT).
- Cooperación (Art. 19.14 del T-MEC y 14.15 del TIPAT).
- Servicios informáticos interactivos (Art. 19.17 del T-MEC).

Asimismo, el T-MEC incluye un Anexo Sectorial de Tecnología de la Información y de la Comunicación (Anexo 12-C), que contiene definiciones y artículos relacionados a ciberseguridad; por ejemplo:

- Definiciones de algoritmo criptográfico, clave, criptografía y encriptación.
- Artículo 12.C.2: Productos TIC que utilizan Criptografía.
- Artículo 12.C.4: Actividades de Cooperación Regional en Equipos de Telecomunicaciones.

Finalmente, el Capítulo 11 del T-MEC: Obstáculos Técnicos al Comercio, incluye una serie de artículos relativos a la elaboración, adopción y aplicación de normas, reglamentos técnicos y procedimientos de evaluación de la conformidad, que deberán también considerarse, acotados, en el marco jurídico y propuestas legislativas en materia de ciberseguridad.

V. Seguridad Nacional y fuerzas armadas

Diferenciar funciones y responsabilidades en ciberseguridad y ciberdefensa:

- Las actividades relacionadas con la ciberdefensa deben ser debidamente acotadas conforme a las facultades de los diferentes cuerpos de seguridad involucrados en la atención a estos casos, considerando las diferentes áreas de

responsabilidad. Esto es, la ciberdefensa debe tener su propio marco jurídico y conceptual, teniendo la precaución de no sobre regular.

- Los cibercrímenes pueden afectar de manera directa la confidencialidad, integridad y disponibilidad de la información, sistemas informáticos, redes de telecomunicaciones, sistemas de procesos automatizados y control (IoT), aplicativos diversos, proveeduría de servicios de Internet e intermediarios, entre otros, por lo cual se pueden ver afectadas instituciones gubernamentales y personas físicas y morales del sector privado y ciudadanos en general. Así, deben mantenerse los mecanismos de colaboración determinados por la autoridad para la colaboración del sector privado en la atención a estos casos, a fin de que los proveedores de servicio de Internet y otros intermediarios, como proveedores de servicios en línea (Online), no sean vistos como corresponsables de la comisión de estos delitos, en tanto que son proveedores de la conectividad y otros servicios, no de su uso, ni de sus contenidos.

- Debe estar limitada claramente la responsabilidad de cada parte que interviene con base al servicio que se ofrece; por ello las entidades intermediarias deberían tener la responsabilidad de incorporar factores de autenticación para realizar diferentes operaciones que validen la identidad de las partes que intervienen en el servicio. Por lo tanto, los proveedores de conectividad son una vía para que funcionen los servicios, pero son los prestadores de éstos últimos los responsables finales de resguardar la seguridad de la transacción con verificaciones específicas.