CERC.
Consejo de Expertos en Regulación y Ciberseguridad

Consejo de Expertos en Regulación y Ciberseguridad

Recomendaciones a las Iniciativas de Ley en Materia de Ciberseguridad

INTRODUCCIÓN

- ¿Tiene la ciudadanía confianza en el espacio digital?
- ¿Qué va más rápido, la tecnología o las leyes?
- ¿Sabías que actualmente se encuentran cuatro iniciativas en el Congreso que buscan crear leyes sobre ciberseguridad?
- ¿Sabías que México no se ha adherido al Convenio de Budapest de 2001?
- ¿Cuál es la agenda del Poder Legislativo en materia de ciberseguridad?
- ¿El alcance las iniciativas actuales en materia de ciberseguridad corresponden a las necesidades que presentan las TICs?
- ¿Existe un punto de encuentro entre estas iniciativas respecto a los avances de otros países en la materia?

ACRÓNIMOS

- **JLT:** Sen. Jesús Lucía Trasviña Waldenrath
- **JSN:** Dip. Javier Salinas Narváez
- **MAM:** Sen. Miguel Ángel Mancera Espinosa
- **LSI:** Ley de Seguridad Informática
- **LGC:** Ley General de Ciberseguridad
- **UIT:** Unión Internacional de Telecomunicaciones
- **NIST:** Instituto Nacional de Estándares y Tecnología (por sus siglas en inglés, National Institute of Standards and Technology).
- **ENISA:** Agencia Europea de Seguridad de las Redes y de la Información (por sus siglas en inglés, European Union Agency for Cybersecurity).
- **ISACA:** Asociación de Auditoría y Control de Sistemas de Información (por sus siglas en inglés, Information Systems Audit and Control Association).
- **IEC:** Comisión Electrotécnica Internacional (por sus siglas en inglés, International Electrotechnical Commission)
- **ISO**: Organizacion Internacional para Estandarización(por sus siglas en inglés, International Organization for Standardization)
- **NCSC UK**: Centro Nacional de de Ciberseguridad del Reino Unido (por sus siglas en inglés, National Cyber Security Centre United Kingdom)
- **NICCS**: Iniciativa Nacional para Carreras Profesionales y Estudios en Ciberseguridad (por sus siglas en inglés, National Initiative for Cybersecurity Careers and Studies)
- **NIPP**: Plan de Protección a Infraestructura Nacional (por sus siglas en inglés, National Initiative for Cybersecurity Careers and Studies)

DEFINICIONES

CIBERSEGURIDAD

JLT LGC

La ciberseguridad es una función a cargo de la Federación, las Entidades Federativas y Municipios que tiene como fines salvaguardar el uso seguro y responsable de las redes, los sistemas de información y comunicaciones [...] (Art. 2)

Se reduce la ciberseguridad a una función exclusiva de las autoridades.

JSN

Capacidad del Estado Mexicano para implementar políticas, normas, procedimientos, medidas y controles asociados con la protección de activos de información y de TIC de la sociedad, gobierno, economía y Seguridad Nacional en el ciberespacio. (Art. 6, frac. XV)

Se limita a considerar a la ciberseguridad como una capacidad del Estado mexicano.

MAM

Todas las actividades o acciones necesarias para la protección de las redes y sistemas de información, de las personas usuarias de tales sistemas y de otras personas afectadas por las amenazas a la seguridad. (Art. 2, frac. III)

Solamente toma en cuenta las afectaciones a las personas.

UIT:"El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y usuarios en el ciberentorno".

No existe consenso respecto a la definición de ciberseguridad. Las diferencias en definiciones denotan la necesidad de discutir si la materia de ciberseguridad es exclusiva del Estado. El grado de amplitud de la definición pudiera generar preocupaciones. Se recomienda tomar en consideración las definiciones propuestas o adoptadas por otros actores y foros internacionales.

CIBERAMENAZA

JLT LSI Y LGC

Riesgo potencial relacionado a las vulnerabilidades de los sistemas informáticos y de infraestructura física y pasiva de las redes públicas de telecomunicaciones de permitir causar daño a los procesos y continuidad de las infraestructuras críticas de información, las infraestructuras de información esenciales, así como la seguridad de las personas. (Art. 4, frac. VI)

Las ciberamenazas se relacionan más con las vulnerabilidades de infraestructura activa con elementos como antenas, cableado, servidores, routers, endopoints, y más.

JSN

Amenaza emergente con capacidad de provocar un efecto adverso en o desde el ciberespacio, y está relacionado a las vulnerabilidades de las personas, los procesos críticos y las TIC de los sujetos obligados. (Art. 6, frac. VI)

No se define qué es un efecto adverso.
No se define cuáles son las vulnerabilidades de las personas.

MAM

Cualquier situación potencial, hecho o acción que pueda amenazar, dañar, eliminar, modificar, perturbar, negar o afectar desfavorablemente de otra manera las redes y los sistemas de información, a las personas usuarias de tales sistemas y a otras personas que puedan resultar afectadas. (Art. 2, frac. IV)

A la definición le hace falta referir los medios a través de los cuales se cometen las ciberamenazas tales como los sistemas de información o el mundo virtual como medio y/o fin para la afectación.

NCSC UK: "Intentos maliciosos de dañar, interrumpir u obtener acceso no autorizado a sistemas, redes o dispositivos informáticos, a través de medios cibernéticos."

CIBERDELITO

JLT LSI Y LGC

Acciones delictivas que utilizan como medio o fin a las tecnologías de la información y comunicación y que se encuentran tipificados en algún código penal u otro ordenamiento nacional. (Art. 6, frac. XXI)

JSN

Conductas delictivas perpetradas en o desde el ciberespacio utilizando las TIC como medio o fin y que se encuentran tipificados en la legislación nacional y/o legislación internacional aplicable. (Art. 6, frac. IX)

MAM

Amenaza a la seguridad nacional. Actos tendentes a amenazar, afectar, inhabilitar o destruir la infraestructura activa o pasiva de telecomunicaciones que sean indispensables para la provisión de bienes o servicios públicos o para el adecuado funcionamiento de las instituciones del Estado. (Art. 6, frac. VI)

Los ciberdelitos pueden afectar directamente la confidencialidad, integridad y disponibilidad de la información, los sistemas informáticos, redes de telecomunicaciones, entre otros. Estos no están relacionados solamente con acciones que afecten la funcionalidad del Estado, sino también en las dimensiones sociales y privadas.

INTERPOL: "Delitos cometidos contra datos informáticos, medios de almacenamiento de datos informáticos, sistemas informáticos, proveedores de servicios."

Es acertado incluir la legislación internacional para sentar la base de una futura cooperación internacional por parte de México en ciberseguridad.

CIBERDEFENSA

JLT LSI Y LGC

Conjunto de acciones, recursos y mecanismos del estado en materia de seguridad nacional para prevenir, identificar y neutralizar toda ciber-amenaza o ciber-ataque que afecte a la infraestructura crítica nacional. (Art. 4, frac. VIII)

JSN

Capacidad del Estado Mexicano traducida en acciones, recursos y mecanismos de seguridad y defensa nacional en el Ciberespacio, gestionada a través de las instancias de Seguridad Nacional. (Art. 6, frac. VIII)

MAM

Conjunto de acciones, recursos y mecanismos en materia de seguridad para prevenir, identificar, reaccionar y neutralizar las amenazas, ciberamenazas o ciberataques. (Art. 2, frac. V)

La ciberdefensa no es una capacidad exclusiva de los Estados ni es el único actor posiblemente afectado, ya que este ámbito involucra a toda la comunidad del ecosistema digital. Se debe apegar a los conceptos homologados internacionalmente, así como la participación ciudadana para definir las instancias que gestionen la ciberdefensa.

Una "amenaza" es un término muy amplio.

Se recomienda eliminar el concepto de "amenazas".

LEY Nº 30999 Perú: "Entiéndase por ciberdefensa a la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional."

Considerar la conveniencia de no limitar la ciberdefensa a actores puramente estatales.

CIBERATAQUE

JLT LGC

Acción realizada a través de uno o varios sistemas informáticos con el objeto de amenazar, afectar, inhabilitar, destruir, vulnerar, eliminar, negar o modificar la información contenida en un sistema de información, bases de datos y/o registro digital. (Art. 6, frac. XII)

JSN

Acción voluntaria ofensiva o maliciosa en o desde el ciberespacio con la intención de causar un efecto adverso a las Tecnologías de Operación (TO) de las Infraestructuras Críticas de Información e infraestructuras de información esenciales, así como cualquier situación que ponga en peligro inminente a la Seguridad Nacional a través del Ciberespacio. (Art. 6, frac. VII)

MAM

Acción realizada a través de uno o varios sistemas informáticos con el objeto de amenazar, afectar, inhabilitar, destruir, vulnerar, eliminar, negar o modificar la información contenida en un sistema de información, bases de datos y/o registro digital. (Art. 2, frac. II)

No hace mención explícita sobre una "intención maliciosa" como motivación de un ciberataque.

Considerar el ámbitos en los que pueden ocurrir los ciberataques además de las acciones que ponen en peligro la seguridad nacional. No hace falta calificar a la acción de "ofensiva o maliciosa"

No hace mención explícita sobre una "intención maliciosa" como motivación de un ciberataque.

NIST: "Un ataque, a través del ciberespacio, dirigido al uso del ciberespacio por parte de una empresa con el propósito de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno / infraestructura informática; o destruir la integridad de los datos o robar información controlada."

Es importante considerar que otros actores como personas, organizaciones o empresas también podrían ser objeto de ciberataques además del estado. Estas acciones deben contener una intención maliciosa para considerarlas como delito, ya que las mismas acciones podrían ser accidentales o contar con el permiso necesario para actuar en ese sentido.

TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

JLT LGC

Equipos de cómputo, programas de computación, servicios y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video. (Art. 4, frac. XX)

JSN

Hardware y/o software que son empleadas por sí solas o dentro de una red para almacenar, procesar, imprimir, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video. (Art. 6, frac. XXIV)

MAM

Equipos de cómputo, programas de computación, servicios y dispositivos de impresión que sean utilizados para almacenar, procesar, con convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video. (Art. 2, frac. XX)

NICCS: "Cualquier tecnología de información, equipo o sistema interconectado o subsistema de equipo que procesa, transmite, recibe o intercambia datos o información."

Homologar la definición conforme a otras referencias acordadas en la agenda internacional, buscando que sea una definición que no excluya ningún tipo de tecnología existente o futura.

INTERNET

JLT
LSI Y LGC

Conjunto de redes de telecomunicaciones que a través de la red pública de telecomunicaciones ofertan servicios y comunicaciones digitales. (Art. 4, frac. XV)

MAM

Conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen internet funcionen como una red lógica única. (Art. 2, frac. XIII)

IEC Área 732: Computer network technology: "Red informática mundial y abierta que proporciona varios tipos de servicios de comunicación, utilizando un conjunto común de protocolos especificados para el enrutamiento de paquetes.
1. Estos servicios comprenden principalmente mensajería interpersonal, conferencias informáticas, transferencia de archivos, inicio de sesión remoto, búsqueda de información e inspección de documentos. 2. Los protocolos principales son el protocolo IP y el protocolo TCP, cooperando en la pila TCP / IP. 3. Internet está abierto a cualquier usuario que haya obtenido una dirección IP de un proveedor de servicios de Internet."

Asegurarse que las definiciones que se adopten sean acorde a un concepto global, definiciones internacionalmente aceptadas.

RECOMENDACIONES GENERALES

- Es pertinente hacer una revisión de los enfoques que se dan en algunas iniciativas al reducir la ciberseguridad como una capacidad y respuesta exclusiva del Estado. Este asunto no es una capacidad exclusiva de los Estados, sino que afecta a otros actores e involucre a toda la comunidad del ecosistema digital.

- La agenda de ciberseguridad es un asunto global, por lo que se recomienda homologar las definiciones conforme a las referencias reconocidas en el ámbito internacional, tales como: NIST, ENISA, ISACA y la terminología IEC.

INFRAESTRUCTURA INSTITUCIONAL

JLT LSI

Crear la Agencia Nacional de Seguridad Informática como órgano especializado y dependiente de la Secretaria de Seguridad y Protección Ciudadana, cuyo objetivo central será emitir lineamientos y acciones de prevención e investigación de conductas ilícitas a través de medios informáticos y el monitoreo de Internet, efectuando actividades de ciberinvestigaciones, así como de ciberseguridad en la reducción, mitigación de riesgos de vulnerabilidades, amenazas y ataques cibernéticos que permitan salvaguardar la Seguridad Informática. (Art 3.)

La perspectiva descentralizada podría presentar dificultades de implementación.

JLT LGC

Crear la Comisión Nacional de Ciberseguridad que contará con las instancias, instrumentos, políticas, acciones y servicios para cumplir con los fines de la ciberseguridad. Esta estará presidida por la/el titular de la Secretaría de Seguridad y Protección Ciudadana y en suplencia por el titular de la Agencia Nacional de Ciberseguridad y se integrará por la Conferencia de Seguridad, Conferencia de Ciberdefensa y las Oficinas Estatales de Ciberseguridad. La Agencia Nacional de Seguridad propuesta en la iniciativa LSI será la instancia superior de coordinación y seguimiento a las políticas públicas en materia de ciberseguridad. (Art. 10)

JSN

Plantea la creación de una Plataforma Nacional de Ciberseguridad que será administrada y operada por el Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal.

MAM

Conformación del Centro Nacional de Ciberseguridad (CNC) como parte del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (Art. 7)

- Argentina creó en 2019 el Comité de Ciberseguridad dependiente de la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros. Esta es la entidad encargada de desarrollar las estrategias y mecanismos para la protección de información, servicios y coordinación de gestión de incidentes del país. Los servicios que esta institución provee van desde hacer recomendaciones, capacitación en TICs, alerta sobre vulnerabilidades y proceso de denuncias para delitos informáticos.
- Es similar el caso del Instituto Nacional de Ciberseguridad de España dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Esta entidad concentra la investigación, prestación de servicios y coordinación con los agentes con competencias en materia de ciberseguridad a nivel nacional e internacional.
- A manera de contraste, Estados Unidos realiza un esfuerzo conjunto de agencias, sector público y privado, universidades y sociedad en general para mantener la seguridad cibernética, aún sin contar con una sola agencia especializada responsable de los asuntos en la materia. Muestra de lo anterior, es el Instituto Nacional de Estándares y Tecnología (NIST) el cual creó un Marco de Seguridad Cibernética para establecer normas voluntarias aplicables a las empresas de infraestructura crítica.

- El desarrollo de la infraestructura institucional a la luz de los esfuerzos internacionales es de suma importancia por fungir como garantes para estas leyes.
- Es necesaria una estructura institucional multidisciplinaria con los recursos necesarios y el marco regulatorio pertinente para su eficacia.

TIPIFICACIÓN DE DELITOS COMPARTIDOS

	JLT (LSI) [1]	JLT (LGC) [2]	JSN [3]	MAM [4]
Acceso a sistemas informáticos	✓	✓	✓	✓
Copiar o alterar información	✓	✓	✓	
Alterar el funcionamiento del sistema/Dispositivos tecnológicos	✓	✓	✓	✓
Cause vulnerarbilidades a sistemas informáticos	✓	✓	✓	
Delitos financieros	✓	✓	✓	
Suplantación de identidad	✓	✓	✓	
Acoso, trata y pornografía infantil	✓	✓	✓	✓
Propiedad intelectual	✓	✓		✓
Estafa, fraude y espionaje	✓	✓		✓
Acceso y uso indebido de datos personales	✓	✓		
Afectación a infraestructuras críticas o del Estado		✓	✓	✓

*El listado se compone de los delitos que se compartan entre dos o más legisladores.

TIPIFICACIÓN DE DELITOS EXCLUSIVOS

JLT
LSI

- Incitación a la Violencia y Alteración del Orden Social.
- Delitos contra la Imagen Personal.
- Grooming.
- Turismo Sexual.
- Lenocinio.

JSN

- Delitos por sujetos obligados de carácter público:
- No implementar las medidas y controles contenidos en la ley.
- No gestionar la plataforma Nacional de Ciberseguridad.
- No dar aviso inmediato de incidentes.
- Transmitir información confidencial.
- Delitos por sujetos obligados de carácter privado:
- Incumplir acuerdos de seguridad con proveedores de activos de TIC.
- Instalación de hardware o software malicioso.
- No darse de alta en la Plataforma Nacional.
- No permitir la verificación de las autoridades investigadoras de delitos.

MAM

- Instalación de programas informáticos maliciosos.
- Crear, operar, controlar o administrar sitios de internet falsos.
- Utilización de sistemas informáticos para buscar, generar y aprovechar vulnerabilidades sin autorización.
- Afectaciones a la disponibilidad, integridad y confidencialidad de los datos o sistemas de infraestructura informática, crítica o del Estado.

- Los delitos deben estar delimitados y descritos adecuadamente, con la cautela de dejar la flexibilidad suficiente para situaciones que pudieran considerarse tendientes a un delito.
- La "suplantación de identidad" puede ser de tres maneras y es necesario incluirlas en su tipificación como delito: a) se encuentran los datos de una persona en el ciberespacio y son usados para suplantar a esa persona en el ciberespacio; b) se encuentran los datos de una persona en el mundo real y son usados para suplantar a esa persona en el ciberespacio; y c) se encuentran los datos de una persona en el ciberespacio y son usados para suplantar a esa persona en el mundo real.
- Establecer específicamente la intención que motiva a las acciones que pueden llevar a cometer los delitos que se tipifican. Es decir, el delito se comete cuando no se cuenta con autorización para llevar a cabo la afectación y cuando contenga la intención de afectar maliciosamente los sistemas o información.
- La iniciativa LGC de la Senadora Trasviña establece la Incitación a la Violencia y Alteración del Orden Social como delito. Esto presenta un riesgo a la protección de personas a su derecho a la libertad de expresión, por contener delimitaciones con términos como "hostilidad" o "discriminación" (Art. 32), y que en todo caso parecen cuestiones que se han venido atendiendo mediante políticas privadas de los proveedores del servicio.

El Convenio de Budapest promueve la cooperación internacional para perseguir una política criminal común enfocada en proteger a la sociedad contra el cibercrimen. Hasta ahora son 66 los países miembros: Argentina, Canadá, Chile, Estados Unidos, la Unión Europea, Israeñ, Filipinas, Japón y Sri Lanka, entre otros.

Si México se adhiere al Convenio de Budapest de 2001, se vería beneficiado de la habilitación de la construcción de ciberseguridad mediante: 1) la tipificación de cibercrímenes y el renovar la definición de los delitos existentes que se han transformado con el uso de tecnologías; y 2) establecer una colaboración transnacional que habilita la estandarización en métodos de investigación y respuesta ante la cibercriminalidad, lo que sin duda es un elemento clave en el combate a los ciberdelitos.

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD (ENC)

JLT
LSI

Propone la creación una nueva ENC como documento que establece la visión, principios y objetivos del Estado Mexicano alineados a las prioridades en materia de ciberseguridad. Implica el desarrollo, implementación, medición y seguimiento de planes y acciones de la visión de un gobierno en materia de ciberseguridad. (Art 6, fracc XXIX)

JSN

Reconoce la ENC del 2017 e indica que La Comisión Intersecretarial para el Desarrollo de Gobierno Electrónico será responsable de mantenerla actualizada y dar seguimiento a su implementación. (Art. 7)

MAM

Plantea que el Centro Nacional de Ciberseguridad contará con una Estrategia Nacional de Ciberseguridad que será actualizada al menos cada dos años. Esta estrategia sería el instrumento mediante el cual se llevará a cabo la coordinación de las autoridades federales, estatales y locales en materia de ciberseguridad. (Art 17 y 36)

Cualquiera que sea el mecanismo de estrategia lo más importante es que tome en cuenta a los actores involucrados en la toma de decisiones y la cooperación entre los diferentes sectores, así como un enfoque en el cuidado de infraestructuras críticas, gestión de riesgos, concientización y cultura de la ciberseguridad y el poder añadir normas y estándares con la intención de mantener la seguridad de los sistemas informáticos que pueden ser más afectados.

Por lo menos quince países de América Latina están desarrollando o ya cuentan con estrategias nacionales de ciberseguridad, mientras que en otros países el enfoque es distinto.

Estados Unidos considera a la seguridad de la información como una prioridad abordada desde distintas normas estructuradas y puntuales de distintos sectores: gobierno electrónico, sector financiero, sector salud, información del sector privado y de la población en general. De igual manera, cuentan con distintos estándares en Seguridad de la Información para una gestión de riesgos, mantenimiento, monitoreo, respuesta a incidentes y corrección de daños adecuada a cada situación y sector, además de una penalización muy específica y de contar con diversas agencias especializadas en el área de la seguridad.

La Unión Europea busca la estandarización de operaciones y acciones para que todos sus países miembros la apliquen a través sus propios medios y capacidades. De este modo, se tiene un entendimiento común en el tratamiento de situaciones de crisis o en otras en donde se deban dar a conocer ciertas vulnerabilidades, fallas, falta de controles, brechas de seguridad, y que se puedan identificar y corregir rápidamente.

CONCLUSIONES

- Reconocemos el esfuerzo e interés de los legisladores por promover un marco regulatorio en materia de ciberseguridad, sin embargo, como hemos visto a lo largo de este análisis aún hay camino por andar y la participiación de todos los actores involucrados resulta indispensable.
- Las iniciativas no contemplan en su ámbito algunos temas fundamentales para la ciberseguridad como lo es el tratamiento de los datos personales, la definición de una estrategia que funja como un mecanismo de coordinación incluyente basado en la idea de que la ciberseguridad es un asunto con aspectos de ética que competen a todos los actores.
- No podemos ignorar que la agenda de ciberseguridad es un tema global, en este sentido las políticas públicas que se diseñen deben tomar en cuenta dentro del engranaje institucional, las definiciones y otras disposiciones reconocidas y acordadas a nivel internacional. Las iniciativas deberían promover el que México sea una parte activa en estas discusiones, no solo para recuperarse del rezago que tiene en la materia, sino además para mantener un marco jurídico actualizado aprovechando las mejores prácticas internacionales en ciberseguridad.

ANÁLISIS DE REFERENCIAS

ISO
Una organización no gubernamental que comprende organismos de normalización de más de 160 países con representantes de cada país miembro. Esta organización consolida la visión de diversos países, los miembros colaboran en el desarrollo y promoción de estándares internacionales para tecnología, procesos de pruebas científicas, condiciones de trabajo, problemas sociales y más.

UIT
Es la agencia especializada de las Naciones Unidas responsable de los asuntos relacionados con las tecnologías de la información y comunicación. La estandarización ha sido un aspecto fundamental del mandato de la UIT desde su creación. Las estimaciones sugieren que el 95% del tráfico de comunicaciones internacionales se realiza a través de redes de fibra óptica construidas de conformidad con las normas de la UIT. Los estándares de la UIT son altamente observados y por lo tanto es relevante considerar su recomendación y definiciones.

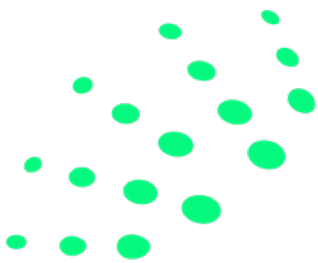
NCSC UK
Es el Centro Nacional de Seguridad Cibernética del Reino Unido que aconseja y apoya a los sectores público y privado para evitar amenazas de seguridad informática.

NICCS
Es la ventanilla única del gobierno de Estados Unidos para carreras y estudios de ciberseguridad. Conecta al público con información sobre concienciación en ciberseguridad, programas de grado, formación, carreras y gestión del talento.

NIST
El Instituto Nacional de Estándares y Tecnología es un laboratorio de ciencias físicas y una agencia no reguladora del Departamento de Comercio de los Estados Unidos. Su misión es promover la innovación estadounidense y la competitividad industrial.

Ley N. 30999 Perú
Establece el marco normativo para diferentes entidades del Estado peruano y los institutos militares en el ciberespacio. Es relevante contar con la perspectiva Latinoamericana en el tema de ciberseguridad.

IEC
International Electrotechnical Commission es una organization mundial lider en la preparacion y publicacion de estándares internacionales para tecnologías.



DOCUMENTOS ANALIZADOS

- Iniciativa de Ley de Seguridad Informática de la Senadora Jesús Lucía Trasviña Waldenrath, LXIV Legislatura del Congreso de la Unión de México (2019). Recuperado el 23 de mayo de 2021 de https://infosen.senado.gob.mx/sgsp/gaceta/64/1/2019-03-27-1/assets/documentos/Inic_MORENA_Seguridad_Informatica.pdf
- Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Ciberseguridad de la Senadora Jesús Lucía Trasviña Waldenrath, LXIV Legislatura del Congreso de la Unión de México (2021). Recuperado el 23 de mayo de 2021 de http://sil.gobernacion.gob.mx/Archivos/Documentos/2021/04/asun_4163509_20210406_1616512719.pdf
- Iniciativa que expide la Ley Nacional de Seguridad en el Ciberespacio del Diputado Javier Salinas Narváez (2020). Recuperado el 23 de mayo de 2021 de http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/10/asun_4093498_20201019_1603158505.pdfO
- Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Ciberseguridad del Senador Miguel Ángel Mancera, LXIV Legislatura del Congreso de la Unión de México (2019). Recuperado de https://infosen.senado.gob.mx/sgsp/gaceta/64/3/2020-09-02-1/assets/documentos/Inic_PRD_Sen_Mancera_ciberseguridad.pdf
- Unión Internacional de Telecomunicaciones (UTI). Definición de Ciberseguridad. Recuperada el 23 de mayo de 2021 de: https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf
- International Electrotechnical Commission. (2021). Intranet. Recuperado el 25 de mayo de 2021 de https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=732-07-22
- Gobierno de España. (2019). Estrategia de Ciberseguridad. Recuperado el XX de XXX de 2021 de https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019
- National Institute of Standards and Technology. (2021). Marco de Seguridad Cibernética del Instituto Nacional de Estándares y Tecnología (NIST). Recuperado el 15 de mayo de 2021 de https://www.nist.gov/cybersecurity
- Ministerio de Justicia y Derechos Humanos del Gobierno de Argentina. (2017). Decreto 577/2017 del Gobierno de Argentina mediante el que se crea el Comité de Ciberseguridad. Recuperado el 15 de mayo de 2021 de http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm
- Consejo de Europa. (2021). Convenio de Budapest. Recuperado el 15 de mayo de https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
- Banco Interamericano de Desarrollo (BID). (2020). Ciberseguridad: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe, Reporte Ciberseguridad 2020 (p.10). Recuperado el 23 de marzo de 2021 de: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf