Conceptos y definiciones clave en las leyes internacionales de ciberseguridad

Concepto	Iniciativas en México	Estados Unidos	Unión Europea	Australia	Organismos Multilaterales
Activo	Una persona, estructura, instalación, información y registros, sistemas y recursos de tecnología de la información, material, proceso, relaciones o reputación que tiene valor para quien lo posee, utiliza o administra.	Persona, estructura, instalación, información y registros, sistemas y recursos de tecnología de la información, material, proceso, relaciones o reputación que tienen valor.	Cualquier cosa que tenga valor para la organización, sus operaciones empresariales y su continuidad, incluidos los recursos de información que apoyan la misión de la organización.	Cualquier cosa de valor, como equipos TIC, software o información.	OCDE: Es un depósito de valor que representa un beneficio o una serie de beneficios que obtiene el propietario económico al poseer o utilizar la entidad durante un periodo de tiempo.
Análisis de riesgos	Proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.	El examen sistemático de los componentes y características del riesgo.	Uso sistemático de la información para identificar las fuentes y estimar el riesgo	Valora el impacto potencial de cada riesgo y su probabilidad de ocurrencia.	OAS Definir lo que está en peligro, la magnitud (impacto) del daño causado por una amenaza, las causas o eventos con potencial para causar daño a una infraestructura de TIC y qué hacer frente al riesgo.
Aplicaciones	Programa o conjunto de programas informáticos que realizan el procesamiento de registros para una función específica, diseñado para el beneficio del usuario final.	Un sistema de hardware/software implementado para satisfacer un conjunto particular de requisitos.	N/A	Un programa o grupo de programas informáticos diseñados para usuarios finales.	OCDE: Un servicio digital que facilita las interacciones entre dos o más grupos de usuarios distintos pero interdependientes
Autenticación	Procedimiento para comprobar fehacientemente la identidad de un usuario para acceder a un dispositivo, aplicación, sistema, plataforma o servicio en línea, mediante conocimiento, basado en: información que solo conoce el usuario, pertenencia, basado en algo que posee el usuario, o característica, basada en alguna característica del usuario como datos biométricos.	Proceso de verificación de la identidad u otros atributos de una entidad (usuario, proceso o dispositivo).	Es una forma de comprobar que un usuario es quien dice ser.	Verificación de la identidad de un usuario, proceso o dispositivo como requisito previo para permitir el acceso a los recursos de un sistema.	OEA: Procedimiento que debe seguir un usuario para acceder a los recursos de un sistema o red informática.
Autenticidad	Característica de la seguridad informática que se refiere a la comprobación y confirmación de la identidad real de los activos.	Propiedad conseguida mediante métodos criptográficos de ser genuino y poder ser verificado y fiable, lo que da lugar a la confianza en la validez de una transmisión, información o mensaje, o remitente de información o mensaje.	Propiedad de que una entidad es lo que dice ser.	N/A	N/A
Base de Datos	Recopilación de datos estructurados almacenados de manera digital.	Depósito de información que suele contener información de toda la planta, incluidos datos de procesos, recetas, datos de personal y datos financieros.	N/A	N/A	ITU: Entidad que almacena información del usuario y/o de la red.
Ciberamenaza	Fuente potencial interna o externa a través del Ciberespacio, con capacidad de provocar un funcionamiento incorrecto, pérdida de valor o efecto adverso en los activos.	Cualquier circunstancia o evento con el potencial de afectar negativamente las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización o las personas a través de un sistema de información a través del acceso no autorizado, la destrucción, la divulgación, la modificación de la información y/o la denegación de servicio.	Cualquier circunstancia o evento con el potencial de afectar negativamente a un activo mediante acceso no autorizado, destrucción, divulgación, modificación de datos y/o denegación de servicio.	Cualquier circunstancia o acontecimiento que pueda dañar los sistemas o los datos.	BID: Fuente potencial de perjuicio, externa o interna, a algún activo de la organización que se materializa a través del ciberespacio.
Ciberataque	Cualquier tipo de actividad maliciosa que intente recopilar, interrumpir, denegar, degradar o destruir los recursos del sistema de información o la propia información con la finalidad de afectar la disponibilidad, integridad y confidencialidad del activo.	Cualquier tipo de actividad maliciosa que intente recopilar, interrumpir, denegar, degradar o destruir recursos del sistema de información o la propia información.	Todos aquellos incidentes cibernéticos provocados con intenciones maliciosas en los que se causan daños, perturbaciones o disfuncionalidades.	Un acto deliberado a través del ciberespacio para manipular, perturbar, denegar, degradar o destruir ordenadores o redes, o la información residente en ellos, con el efecto de comprometer gravemente la seguridad nacional, la estabilidad o la prosperidad económica.	BID: Uso deliberado de una ciberarma, por una persona o de manera automática, para causar un daño o efecto perjudicial a un elemento del ciberespacio de un adversario pudiendo tener efectos indirectos en los ámbitos de operaciones convencionales.
Ciberdefensa	Capacidad de un Estado sujeto de derecho internacional traducida en acciones, recursos y mecanismos en materia de Seguridad y Defensa nacionales en el ciberespacio, para prevenir, identificar y neutralizar Ciberamenazas o Ciberataques, incluidos los que atentan contra Infraestructuras Críticas de Información y la seguridad nacional.	Capacidad sincronizada y en tiempo real para descubrir, detectar, analizar y mitigar amenazas y vulnerabilidades.	Se refiere a una variedad de mecanismos defensivos que podrían utilizarse para mitigar o responder a ciberataques.	Inteligencia responsable de las evaluaciones estratégicas y técnicas de inteligencia, utilizadas para asesorar a la defensa y a la toma de decisiones del Gobierno sobre cuestiones de seguridad nacional e internacional,.	BID: Capacidad organizada y preparada para combatir en el ciberespacio. Comprende actividades defensivas, ofensivas y de inteligencia.
Ciberespacio	Entorno o ámbito intangible de naturaleza global, soportado por las Tecnologías de la Información y Comunicaciones, en el que se comunican e interactúan las entidades públicas, privadas y la sociedad en general, haciendo uso del ejercicio de sus derechos y libertades.	Dominio global dentro del entorno de la información que consiste en la red interdependiente de infraestructuras de sistemas de información que incluyen Internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados.	Incluye todas las infraestructuras de información accesibles a través de Internet más allá de todas las fronteras territoriales	N/A	N/A

Conceptos y definiciones clave en las leyes internacionales de ciberseguridad

Concepto	Iniciativas en México	Estados Unidos	Unión Europea	Australia	Organismos Multilaterales
Ciberdelito	Acciones u omisiones que constituyen una conducta delictiva donde se utilice como medio o como fin a las tecnologías de la información y comunicación, las que se encuentran tipificadas en un código penal u otro, instrumento internacional o normativa exigible al Estado mexicano. Cualquier actividad ilícita que se comete utilizando medios electrónicos, sistemas informáticos, redes de comunicación o tecnologías digitales, con el objetivo de obtener beneficios económicos, causar daño o vulnerar derechos en el ciberespacio.	Delitos cometidos en Internet o con ayuda de la informática.	Cualquier delito o actividad delictiva facilitada por el ciberespacio o que lo utiliza.	Delitos dirigidos contra ordenadores u otras tecnologías de la información y la comunicación (TIC). Delitos en los que los ordenadores o las TIC son parte integrante de un delito.	OEA: Todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera. (OEA)
Ciberseguridad	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 cualquier organización y usuarios en el ciberespacio. Conjunto de medidas, técnicas y procesos orientados a proteger los sistemas informáticos, redes, dispositivos y datos contra amenazas cibernéticas, garantizando la confidencialidad, integridad y disponibilidad de la información, así como la protección de los activos digitales y la privacidad de los usuarios	Actividad o proceso, habilidad o capacidad, o estado mediante el cual los sistemas de información y comunicaciones y la información contenida en ellos están protegidos y/o defendidos contra daños, uso o modificación no autorizados, o explotación.	La ciberseguridad se refiere a la seguridad del ciberespacio.	Medidas utilizadas para proteger la confidencialidad, integridad y disponibilidad de los sistemas, dispositivos y la información que reside en ellos.	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.
Disponibilidad	Capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.	La propiedad de ser accesible y utilizable bajo demanda.	El hecho de que los datos sean accesibles y los servicios estén operativos.	La garantía de que los sistemas y la información son accesibles y utilizables por las entidades autorizadas cuando sea necesario.	ITU: Propiedad de los datos o de los recursos de ser accesibles y utilizables bajo demanda por una entidad autorizada.
Dispositivo	Combinación de diversos elementos organizados en circuitos, destinados a controlar y aprovechar las señales eléctricas para cumplir un propósito específico.	Una combinación de componentes que funcionan juntos para servir a un propósito específico.	N/A	N/A	ITU: Es un equipo con las capacidades obligatorias de comunicación y las capacidades opcionales de detección, actuación, captura de datos, almacenamiento y procesamiento de datos.
Entorno Digital	Conjunto de canales, plataformas y herramientas que dispone cualquier individuo, marcas o negocios para tener presencia en Internet.	N/A	N/A	N/A	N/A
Evidencia Digital	Información almacenada en cualquier clase de medio tecnológico que puede ser recolectada y analizada con herramientas y técnicas especiales y ser también utilizada en una investigación o proceso judicial.	Información electrónica almacenada o transmitida en forma binaria.	Información que, por sí sola o en combinación con otros datos, sirve para demostrar un hecho o una acción.	N/A	ITU: Información o datos almacenados o transmitidos en forma binaria, que se ha determinado, a través del proceso de análisis, que son relevantes para la investigación de un incidente de ciberseguridad.
Incidentes de Ciberseguridad o incidentes cibernéticos	Uno o varios eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer o comprometan las operaciones organizacionales y amenazar la seguridad de la información.	Suceso que tiene consecuencias adversas reales o potenciales para (efectos adversos sobre) (supone una amenaza para) un sistema de información o la información que el sistema procesa, almacena o transmite y que puede requerir una acción de respuesta para mitigar las consecuencias.	Evento que se ha evaluado como causante de un efecto real o potencialmente adverso en la seguridad o el rendimiento de un sistema.	Un suceso de ciberseguridad no deseado o inesperado, o una serie de sucesos de este tipo, que tienen una probabilidad significativa de comprometer las operaciones de la empresa.	ITU: Evento cibernético que implica una pérdida de seguridad de la información o afecta a las operaciones comerciales.
Infraestructuras Críticas de Información	Las redes, servicios, equipos e instalaciones asociados o vinculados con activos de Tecnologías de Información y Comunicaciones, y de Tecnologías de Operación TO, cuya afectación, interrupción o destrucción, tendría un impacto en la provisión de bienes y prestación de servicios públicos o privados esenciales que pudieran comprometer la Seguridad Nacional en términos de las leyes en la materia.	Los sistemas y activos, ya sean físicos o virtuales, tan vitales para la sociedad que la incapacidad o destrucción de los mismos puede tener un impacto debilitador en la seguridad, la economía, la salud o la seguridad pública, el medio ambiente o cualquier combinación de estos aspectos.	Infraestructuras de información (redes, hardware, software, etc.) esenciales para el funcionamiento de una nación o un país, como las tecnologías de la información al servicio de los sectores de salud o energía.	Instalaciones físicas, cadenas de suministro, tecnologías de la información y redes de comunicación que, si se destruyen, degradan o dejan de estar disponibles durante un periodo prolongado, repercutirían significativamente en el bienestar social o económico de la nación, o afectarían a la capacidad de una nación para llevar a cabo la defensa nacional y garantizar la seguridad nacional.	OEA: Los sistemas y activos, ya sean físicos o virtuales, tan vitales para la sociedad que la incapacidad o destrucción de los mismos puede tener un impacto debilitador en la seguridad, la economía, la salud o la seguridad pública, el medio ambiente o cualquier combinación de estos aspectos.
Integridad	Propiedad de la información, por la que se garantiza la exactitud de los datos transmitidos o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.	Propiedad por la cual la información, un sistema de información o un componente de un sistema no ha sido modificado o destruido de forma no autorizada.	La confirmación de que los datos enviados, recibidos o almacenados están completos y no se han modificado.	La garantía de que la información ha sido creada, modificada o suprimida únicamente por personas autorizadas.	ITU: La propiedad de que los datos no han sido alterados o destruidos de forma no autorizada.
Malware	Cualquier tipo de software malicioso diseñado para infiltrarse o dañar un sistema informático, dispositivo electrónico, red de computadoras o cualquier otro sistema digital, sin el consentimiento del usuario y con el propósito de causar daño, robar información, o comprometer la seguridad y el funcionamiento del sistema afectado.	Software que compromete el funcionamiento de un sistema al realizar una función o proceso no autorizado.	Programa no autorizado que se inserta en un sistema informático y luego se propaga a otros ordenadores a través de redes o discos.	Software malicioso utilizado para obtener acceso no autorizado a ordenadores, robar información e interrumpir o inutilizar redes.	ITU: Nombre genérico del software que realiza intencionadamente acciones que pueden dañar los datos o perturbar los sistemas.

Conceptos y definiciones clave en las leyes internacionales de ciberseguridad

Concepto	Iniciativas en México	Estados Unidos	Unión Europea	Australia	Organismos Multilaterales
Medio de almacena-miento informático	Dispositivo que escribe y lee datos digitales en un soporte de forma temporal o permanente, siendo su funcionamiento de tipo mecánico o electrónico.	N/A	N/A	N/A	ITU: Dispositivo situado en la parte central de un sistema de videovigilancia. Se utiliza para recuperar, almacenar medios y proporcionar una capacidad de servicio de transmisión de medios.
Riesgo	La probabilidad de que una amenaza aproveche una vulnerabilidad y cause un determinado impacto, pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información.	El potencial de un resultado no deseado o adverso resultante de un incidente, evento o suceso, determinado por la probabilidad de que una amenaza concreta explote una vulnerabilidad concreta, con las consecuencias asociadas.	La posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y cause así daños a la organización.	N/A	ONU: La probabilidad de que un resultado tenga un efecto negativo sobre las personas, los sistemas o los activos.
Seguridad de la Información	La capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, trazabilidad y no repudio de la misma.	La protección de la información y los sistemas de información frente al acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados, con el fin de proporcionar confidencialidad, integridad y disponibilidad.	Preservación de la confidencialidad, integridad y disponibilidad de la información. Además, pueden intervenir otras propiedades, como la autenticidad, la rendición de cuentas, el no repudio y la fiabilidad.	Protección de la información y los sistemas de información frente al acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados, con el fin de garantizar la confidencialidad, integridad y disponibilidad.	ITU: Seguridad preservación de la confidencialidad, integridad y disponibilidad de la información.
Sistema de Información o Sistema Informático	Conjunto de aplicaciones, servicios, activos u otros componentes para el almacenamiento y procesamiento de datos o información.	Conjunto diferenciado de recursos de información organizados para la recopilación, el tratamiento, el mantenimiento, el uso, la puesta en común, la difusión o la eliminación de información.	Conjunto de componentes tecnológicos relacionados que trabajan juntos para dar soporte a un proceso de negocio o proporcionar un servicio.	Conjunto relacionado de hardware y software utilizado para el procesamiento, almacenamiento o comunicación de información y el marco de gobernanza en el que opera.	ITU: Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan información.
Sistema o medio Telemático	Medio que combina los sistemas de telecomunicaciones e informáticos como método para transmitir datos o información.	N/A	N/A	N/A	ITU: Servicios de telecomunicación suplementarios a los servicios telegráficos o telefónicos convencionales, que generalmente utilizan técnicas de teleproceso para permitir a un usuario recibir o enviar información pública o privada, o efectuar operaciones como consultas de archivos, reservas, transacciones comerciales o bancarias.
Software	Conjunto de programas, instrucciones y datos que permiten a un sistema informático realizar diversas tareas, operaciones y funciones de manera automatizada y controlada.	Programas informáticos y datos asociados que pueden escribirse o modificarse dinámicamente durante su ejecución.	N/A	Conjunto de datos o instrucciones que indican a un ordenador cómo debe funcionar.	ITU: Programas informáticos, procedimientos, reglas y cualquier documentación asociada relacionada con el funcionamiento de un sistema.
Tecnología para Intervención legal de comunica-ciones	Todo equipo, herramienta, medio, dispositivo, o software diseñados o modificados específicamente para interceptar, monitorear, registrar o manipular las comunicaciones electrónicas.	N/A	N/A	N/A	N/A
Telecomuni-caciones	Toda emisión, transmisión o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos, sin incluir la radiodifusión.	La transmisión, entre puntos especificados por el usuario, de información de su elección, sin modificar la forma ni el contenido de la información enviada y recibida.	N/A	N/A	ITU: Toda transmisión, emisión o recepción de signos, señales, escritos, imágenes y sonidos o inteligencia de cualquier naturaleza por hilo, radio, medios ópticos u otros sistemas electromagnéticos
Usuario	Persona o entidad autorizada para acceder a un sistema de información.	N/A	N/A	Persona autorizada a acceder a un sistema.	ITU: Cualquier entidad externa a la red que utiliza conexiones a través de la red para comunicarse.
Vulnerabilidad	Estado o situación de un activo que permite que una amenaza afecte la confidencialidad, integridad y disponibilidad del mismo.	Una característica o debilidad específica que hace que una organización o activo (como la información o un sistema de información) esté abierto a ser explotado por una amenaza determinada o susceptible a un peligro concreto.	La existencia de una debilidad, diseño o error de implementación que puede conducir a un evento inesperado e indeseable que comprometa la seguridad del sistema informático, red, aplicación o protocolo involucrado.	Debilidad en los requisitos de seguridad, el diseño, la implementación o el funcionamiento de un sistema que podría activarse accidentalmente o explotarse intencionadamente y dar lugar a una violación de la política de seguridad del sistema.	ITU: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

CERC Consejo de Expertos en Regulación y Ciberseguridad

Regulación Internacional e iniciativas en México sobre **Ciberseguridad**

global.alliances@metabaseq.com
+52 55 2211 0920

// Better Base, Better Future