IoT Security Institute capitulo Chile

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 1.	La presente norma técnica tiene por objeto establecer un marco regulatorio que comprenda los fundamentos generales de ciberseguridad en base a los cuales deben diseñarse, instalarse y operarse las redes y sistemas utilizados para la prestación de servicios de telecomunicaciones por parte de aquellos titulares de concesión o permiso que hayan sido declarados como operadores relevantes por esta Subsecretaría. De igual manera, esta norma técnica busca normar el envío de información sobre ciberincidencias que los concesionarios y permisionarios de servicios de telecomunicaciones deban reportar a la Subsecretaría, con el objeto de coordinar las acciones orientadas mitigar sus efectos y contribuir a una oportuna restitución de los servicios afectados. Serán parte de las actividades normadas por el presente documento todas aquellas soluciones o servicios que se encuentren vinculadas con actividades tales como: • Análisis de Datos (Big Data) • Internet de las Cosas • Cadena de bloqueo (Blockchain)

	• Computación cognitiva • Smart Administration • Smart Health • Smart cities • Smart Farming • Smart house • Smart car • Smart grid • Smart building • 5G De igual manera, será aplicable la normativa a cualquier actividad que sea generada por los concesionarios y permisionarios de servicios de telecomunicaciones que tenga vinculación con la lista antes facilitada.
Artículo 2.	Incidente de seguridad Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

	Informática forense La informática forense consiste en un proceso de investigación de los sistemas de información para detectar toda evidencia que pueda ser presentada como prueba fehaciente en un procedimiento judicial. Para esta investigación se hace necesaria la aplicación de técnicas científicas y analíticas especializadas que permitan identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Entre las técnicas mencionadas se incluyen reconstruir el sistema informático, examinar datos residuales y explicar las características técnicas del uso aplicado a los datos y bienes informáticos. Integridad La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones claves en la seguridad de la información, ya que de un lado, se pretende evitar los accesos no auto- rizados a los datos, y de otro, se garantiza la no alteración de los mismos.

	Inyección SQL Es un tipo de ataque que se aprovecha de una vulnerabilidad en la validación de los contenidos introducidos en un formulario web y que pue- de permitir la obtención de forma ilegítima de los datos almacenados en la base de datos del sitio web, entre ellos las credenciales de acceso. Sinónimo de SQL Injection IoT La abreviatura de “Internet of Things” (Internet de las Cosas en inglés) representa todos los objetos de uso diario que utilizan internet para ofrecer una experiencia más completa y la conexión entre dispositivos. Por ejemplo, las pulsera de seguimiento cardíaco se conectan a la red y también pueden vincularse con los smartphones, etc.
Artículo 3.	Serán parte de las actividades normadas por el presente documento todas aquellas soluciones o servicios que se encuentren vinculadas con actividades tales como: • Análisis de Datos (Big Data) • Internet de las Cosas • Cadena de bloqueo (Blockchain)

	• Computación cognitiva • Smart Administration • Smart Health • Smart cities • Smart Farming • Smart house • Smart car • Smart grid • Smart building • 5G De igual manera, será aplicable la normativa a cualquier actividad que sea generada por los concesionarios y permisionarios de servicios de telecomunicaciones que tenga vinculación con la lista antes facilitada.
Artículo 6.	Roles del equipo de trabajo de la Ciberseguridad Todo operador relevante deberá contar permanentemente con una debida estructura y equipo de trabajo el cual tenga como funciones la correcta función del resguardo de las actividades de ciberseguridad por parte de los concesionarios y permisionarios de servicios de telecomunicaciones. Los

	integrantes del equipo deberán poseer las competencias suficientes para identificar los riesgos de afectación de los servicios de telecomunicaciones por causa de ciberincidencias, verificar el cumplimiento eficaz de los respectivos planes de gestión, reportar las ciberincidencias y coordinar la gestión ciberseguridad con las autoridades competentes. Los operadores relevantes deberán informar a Subtel, en el plazo que se instruya, las identidades de sus encargados de ciberseguridad, la unidad a la que pertenecen y los medios de contacto pertinentes, informando oportunamente en caso que exista alguna modificación al respecto. Entre los roles que deberán contar los concesionarios y permisionarios de servicios de telecomunicaciones deben estar: • CSA (Chief Security Ambassador): este puesto es creado para promover, difundir y concienciar sobre aspectos relativos a la ciberseguridad, exponiendo a las empresas la necesidad de estar preparadas y también mostrando las diferentes capacidades que deben incorporar para afrontar los numerosos riesgos y amenazas que las acechan. • Analista de seguridad: son los individuos que están en los equipos de monitorización del SOC, revisando eventos de seguridad y alertas, realizando un análisis de las mismas, y cuando aplica, escalando las alertas que resultan incidentes a los especialistas de "incidencias". Es decir, están en constante

	detección de cualquier posible vulnerabilidad técnica en los sistemas informáticos y redes de la compañía. • Arquitecto de seguridad: es el responsable de asegurar todos los desarrollos que se realicen en el entorno y la organización, para ello, previamente diseña la arquitectura de ciberseguridad. • Especialista forense: es el encargado de realizar un análisis detallado de las redes y sistemas tras sufrir un incidente de seguridad o ciberataque. • Especialista en incidencias: cuando se produce un ataque de seguridad, es el responsable de coordinar las actividades que se deben de realizar para solventar este ataque. Activará el plan de control para que todos los equipos trabajen alineados y las incidencias sufridas tengan el menor impacto posible. Los roles antes mencionados tendrán entre sus obligaciones las actividades indicadas en su descripción y no podrán cumplir un doble rol en los concesionarios y permisionarios de servicios de telecomunicaciones en tareas de protección de los datos y la seguridad de la Información los cuales deberán contar con personal acorde para cubrir cada uno de los ámbitos de forma independiente. Los operadores relevantes deberán informar a Subtel, en el plazo que se instruya, las identidades de sus encargados de ciberseguridad, la unidad a la que pertenecen y los medios de contacto

	pertinentes, informando oportunamente en caso que exista alguna modificación al respecto.
Artículo 7.	Los organismos públicos o empresas privadas obligadas a notificar un ciberincidente bajo alguna regulación, deberán notificar aquellos ciberincidentes acaecidos en su infraestructura tecnológica que se encuadren dentro del ALCANCE DE LA NORMA, los NIVELES DE PELIGROSIDAD y los NIVELES DE IMPACTO referenciados en el presente documento. De igual forma podrán reportar otros ciberincidentes o ciberamenazas que considere oportuno, atendiendo a los siguientes criterios: Necesidad o conveniencia para el organismo de contar con el apoyo del CSIRT de referencia para la investigación o resolución de ciberincidentes. Beneficios o interés general para la seguridad del conjunto de la comunidad de ciberseguridad, así como para el aumento de la toma de consciencia situacional del estado de la ciberseguridad a nivel estatal por parte de los organismos públicos competentes.
Artículo 8.	CRITERIOS PARA LA NOTIFICACIÓN

	Para la notificación de los incidentes de ciberseguridad se utilizará como criterio de referencia el Nivel de peligrosidad que se asigne a un incidente, sin perjuicio de que a lo largo del desarrollo, mitigación o resolución del mismo, se categorice con un determinado Nivel de impacto que haga aconsejable la comunicación del incidente a la autoridad competente o CSIRT de referencia. En todo caso, cuando un determinado suceso pueda asociarse a más de un tipo de incidente contenido en la Ilustración 4. Clasificación/Taxonomía de los ciberincidentes, debido a sus características potenciales, éste se asociará a aquel que tenga un Nivel de peligrosidad superior de acuerdo a los criterios expuestos en este apartado. Nivel de peligrosidad del ciberincidente El indicador de peligrosidad determina la potencial amenaza que supondría la materialización de un incidente en los sistemas de información o comunicación del ente afectado, así como para los servicios prestados o la continuidad de negocio en caso de haberla. Este indicador se fundamenta en las características intrínsecas a la tipología de amenaza y su comportamiento.

	Los incidentes se asociarán a alguno de los siguientes niveles de peligrosidad: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO.