ASHA SOLUTION SPA

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 2.	En la definición de "Ciberespacio", entendemos que se refiere a los servicios públicos y, en ese caso, nos parece que debe explicitarse que se trata del acceso a Internet, en sus componentes nacional (p.e PIT) e internacional. La actividad de los cibercriminales se desarrolla sobre la Internet "superficial" y la "Deep Web o Dark Web" que corren por una misma infraestructura, pero con mecanismos tecnológicos que permiten ocultar la identidad y el accionar de los cibercriminales en el segundo caso. Su objetivo es, a través de la red pública de Internet, poder acceder a los activos de información de empresas, entidades y consumidores finales, almacenados en centros de datos, computadores personales y teléfonos móviles principalmente. En otros casos, se trata de afectar la disponibilidad de la infraestructura crítica de un operador de telecomunicaciones, una empresa o institución pública o privada, mediante ataques de denegación de servicios, desde múltiples servidores distribuidos en la Internet. Es este el contexto en el que actúan los "CSIRT" o "CERT", si se opta por la certificación de la Carnegie Mellon University en Pittsburgh, quien estableció el primer centro de respuesta a incidente en el año 1988. Por estas razón nos parece importante explicitar en esta definición a la red

	Internet pública.
Artículo 4.	Consistente con lo anterior, un operador relevante comercializa el servicio de acceso a Internet como parte de su oferta comercial básica y, opcionalmente, todas las prestaciones de valor agregado que se implementan sobre la Internet pública, tales como TV, telefonía, redes sociales, etc. Por esta razón, el operador relevante es un ISP (Internet Service Provider), lo que implica que forma parte de una jerarquía de ISPs, partiendo por los denominados Tier 1 (mayoristas globales), los Tier 2 (distribuidores de coberturas regionales y/o nacionales) y Tier 3 (revendedores a usuarios finales). Mientras mas alta sea su jerarquía, mas importancia tienen sus capacidades de monitoreo, detección temprana y bloqueo de amenazas. Por lo tanto, creemos que debe agregarse como criterio, para ser declarado relevante, el nivel de jerarquía como ISP y la cantidad de acuerdos de peering que posean. Como extensión de lo anterior, el criterio de operador relevante debiera aplicarse para los ISP Tier 1 y 2 pues, aunque usualmente no alcanzan directamente a usuarios finales, un ciberataque a través de ellos y sus interconexiones de peering con otros ISP si podría conseguirlo. Como iniciativa, convendría analizar la implementación de un CERT sectorial para todos los operadores relevantes y/o de Centros de Inteligencia de Amenazas (Threat Intelligence Centers) por operador,

	como se ha hecho en algunos países.
Artículo 7.	Respecto al alcance de los ciberincidentes, cabe aclarar si se reportarán aquellos que no afectan necesariamente a usuarios finales como, por ejemplo, los ataques a los operadores relevantes destinados a robarles ancho de banda Internet o minutos de telefonía. Creemos que sí debería hacerse, pues da cuenta de vulnerabilidades que pueden ser explotadas posteriormente para afectar a clientes finales. En relación a la pérdida de datos personales, la responsabilidad de su protección es compartida entre el operador relevante y el usuario. Por ejemplo, si una base de datos de clientes es robada al operador, la responsabilidad es de éste, pero si se trata de información sensible de un cliente almacenada en servidores de un datacenter del operador, entonces la responsabilidad de incorporar múltiples factores de autenticación o de encriptar datos pudiera ser del cliente final. En consecuencia, cabe aclarar si el reporte de pérdida o exposición de datos personales quedará sujeto a los contratos que definen responsabilidad entre ambas partes o siempre se reportará.
Artículo 12.	En relación a las medidas inmediatas conducentes a la mitigación de los efectos y al restablecimiento de los servicios afectados por una ciberincidencia, los operadores relevantes no solo deberán subsanar las vulnerabilidades de sus sistemas que hubieren permitido o facilitado ciberincidencias, sino también la debida preparación y educación de su personal para evitar que mediante

	ingeniería social se explote una debilidad en la cadena de seguridad del operador.