XAVIER BONNAIRE FAVRE

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 2.	a) Me parece que falta la noción de usuario que también es parte del ciberespacio. b) También falta la noción de usuario. Una ciberincidencia puede resultar de una acción que compromete el uso normal de los sistemas y/o servicios e telecomunicaciones. c) De nuevo falta la noción de usuario final. La ciberseguridad debe asegurar también un mínimo de riesgos y amenazas para los usuarios finales de los servicios. Los riesgos asociados a la ciberseguridad no son solamente relacionados con la infraestructura y los servicios sino que también con los comportamientos de los usuarios de dichos servicios. f) La definición de incidente no me parece adecuada. Un incidente puede tener consecuencias no solamente para las redes y sistemas de información sino que también sobre la seguridad de los usuarios, incluyendo sus datos personales. g) "interrupción, destrucción, corte o fallos" --> agregaría "perturbación" o "degradación". No siempre un incidente tiene consecuencias tan drásticas. Puede

	también generar molestias para los usuarios (degradación de velocidad, tiempo de acceso por ejemplo). i) De nuevo los riesgos no afectan solamente las redes y sistema pero también los usuarios finales. No me parece adecuado hablar de probabilidad de materialización de una amenaza, ya que matemáticamente hablando, eso implica ser capaz de cuantificar precisamente esta probabilidad. Me parece más adecuado hablar de nivel de riesgo (bajo, mediano, alto, crítico) que son nociones discretas más adecuadas en ciberseguridad donde una evaluación probabilística cuantificada es casi imposible en la práctica.
Artículo 3.	De nuevo la noción de usuario está totalmente ausente de esta definición, lo que no me parece adecuado. El texto da la impresión que el ciberespacio se resume a un problema técnico y de infraestructura, cuando en la realidad la parte social y el comportamiento del usuario son un facto clave en el diseño y la implementación de políticas de ciberseguridad.
Artículo 5.	No hay obligación de gestionar adecuadamente los riesgos asociados a los usuarios de los servicios. ¿Cuál es la definición de un nivel "adecuado" de ciberseguridad? ¿Cómo se va a fiscalizar?

	b) ¿Qué significa tomar en cuenta el costo de implementación? ¿Si es demasiado costoso, no se implementará? c) Cambiaría por "Evaluación y Gestión ...." e) La noción de continuidad de los servicios me parece una noción muy general. Cada operador puede tener su propia definición de la continuidad y su propia margen de tolerancia. Se necesita dar más detalles o normalizar esta noción. f) También hay que monitorear el comportamiento de los usuarios, no solamente los sistemas. h) ¿Qué pasa si son incompatibles con la ley o la realidad local del país? j) Cambiaría por "Diseño y actualización constante..." k) Se refiere probablemente a casos como el de Huawei (sobre el cual todos los países no están de acuerdo). Me parece que este tema es releva de la Defensa Nacional o del Ministerio de Interior y no de los operadores mismos.

	l) Esta cadena puede verse afectada de forma más o menos severa por decisiones que relevan de la Defensa Nacional y no del operador o proveedor de equipos. Fiscalizar que los operadores cumplan con la norma es necesario pero non suficiente. Hay que generar un mecanismo de certificación de los operadores (eventualmente con varios niveles) para asegurar la calidad de las medidas de ciberseguridad para los usuarios finales.
Artículo 6.	En la terminología internacional, no existe el encargado de ciberseguridad sino un "Oficial de Ciberseguridad". Sugiero adoptar la terminología comúnmente aceptada. ¿Cómo se verificará que el oficial de ciberseguridad tiene las competencias suficientes? ¿Se establecerá un requisito de título o grado mínimo, una experiencia mínima?
Artículo 7.	Es necesario que los operadores usen un estándar internacional que permita no solamente hacer el seguimiento de los incidentes pero también compartir informaciones entre ellos. De este punto de vista, el uso de la plataforma MISP es un estándar internacional que podría ser implementado por la Subtel.

	Tabla de incidencia ---------- Falta un nivel "Ninguna". El modelo internacional NIST define 4 niveles (ninguna, baja, mediana, alta). En algunos casos, un incidente de ciberseguridad no tiene incidencia en el funcionamiento de los servicios pero debe ser declarado y tratado. En algunos casos se puede agregar un nivel "crítica" que corresponde a un incidente que necesita un tratamiento urgente.
Artículo 9.	El informe debería también incluir el mecanismo que usaron los ciberdelincuentes (si se conoce) así que las evidencias recolectadas (malware, logs, etc...). Para eso es necesario una plataforma como MISP. El tiempo mínimo de conservación de los datos relacionados con un ataque me parece insuficiente. Debería ser por lo menos 2 a 3 años. Además, es importante que el operador conserve todos los datos y evidencias, ya que algunos hechos son asunto de la Brigada del Cirbercrimen de la PDI.
Artículo 11.	Hay que consultar a la Brigada del Cibercrimen de la PDI. En algunos casos, la difusión de informaciones, aunque sea un beneficio para los usuarios, podría interferir con investigaciones en curso de

	parte de la PDI.
Artículo 12.	El operador no debería solamente subsanar las vulnerabilidades de los sistemas que hubieron permitido o facilitado un ataque sino que también hacer una auditoría de todos los otros sistemas que podrían presentar el mismo tipo de vulnerabilidades.
Artículo 15.	Me parece muy peligroso que los operadores que no son considerados como relevantes no tengan la obligación de reportar sus incidentes. Debería ser obligatorio para todos para evitar los problemas de ciberseguridad conocidos como "ataques por rebote". Los ataques por rebotes son considerados de alta prioridad por agencias de ciberseguridad muy avanzadas en el tema (la ANSSI en Francia o el INCIBE en España) para los 5 próximos años.
Artículo 16.	Es necesario también implementar medidas que permitan mantener la integridad de las evidencias recolectadas (logs y datos) usando mecanismos de firmas o huellas digitales. El objetivo es asegurar que no puede ocurrir ninguna modificación de estas evidencias en el transcurso de los procedimientos de análisis y recolección.
Artículo 17.	¿Cómo la Subtel lo va a fiscalizar? ¿Tendrán un servicio interno de auditoría? ¿Tendrán una asesoría externa? ¿Tendrán un mecanismo de certificación del nivel de ciberseguridad para cada operador?

Comentarios Generales.	En término general, encuentro que falta el usuario en varias partes del texto. Da un poco la impresión que la ciberseguridad es solamente un asunto técnico relacionado con las redes y los sistemas informáticos. En ninguna parte aparece que los operadores deberían formar a los usuarios de sus servicios a tener un comportamiento seguro. La parte educación es algo fundamental en ciberseguridad. Si los usuarios no están conscientes de los problemas y los operadores no los educan para usar sus servicios de forma correcta, no tendremos ningún avance en ciberseguridad en el país. También encuentro extraño que en ninguna parte se hable de Ingeniería Social. Es un tema muy importante en ciberseguridad que los operadores de telecomunicaciones deberían tomar en cuenta. La formación de todo el personal de los operadores en temas relacionados con la ingeniería social me parece también un punto fundamental que no se menciona en ninguna parte del documento. Xavier Bonnaire Doctor en Informática Responsable linea de Ciberseguridad Departamento de Informática

	Universidad Técnica Federico Santa María.