Héctor Moyano Rojas

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 1.	Desde mi punto de vista, el segundo punto en el objetivo, debería incluir informar las medidas para prevenir y registrar ciberincidencias. La información sobre ciberincidencias sería resultado de los mecanísmos que se implementee
Artículo 2.	En el concepto c) Ciberseguridad: reemplazaría el término riesgo por vulnerabilidad. El riesgo está siempre presente, puede ser mitigado o . Vulnerabilidad es la condición de debilidad o grado de exposición frente al riegso, de un sujeto, objeto o sistema.
Artículo 7.	La obligación de reportar indica los tiempos de acuerdo a la criticacda, entre la detección y reporte. Sin embargo no se establece la obligación de contar con un sistema de monitoreo y análisis de vulnerabilidad, permanente.
Artículo 8.	Los formularios provistos por SANS y otros proveen plantillas estándar, que puede utilizarse o gestionar mediante una plataforma electrónica que permita ingresar, gestionar los reportes, de forma estandarizada, sin demora, en caso de notener servicio quien debe hacer el reporte y de forma autónoma informar, dar seguimiento a los tiempos e involucrados, previamente registrados.
Artículo 9.	El mismo sistema permitiría o plantilla, permitiría asegurrra el contenido de los reportes basado en una plantilla, que puede requerir modificación a la luz de la evolución de los ataques, vectores,

	amenazas e infraestructura que puede ser comprometida.
Artículo 14.	El reporte trimestral debería ser un informe de cumplimiento, para revisar este de acuerdo a los hallazgos o reporte de incidente previo. Los informes trimestrales, debería estar sujetos al minitoreo continuo y análisis de vulnerabilidad las redes, dispositivos y todo aquello que conforma la infraestructura que es parte del servicio.
Artículo 15.	La obligacón de reportar debería aplicar a toda persona, institución u organismo que disponga de infrmación, que permita alertar, prevenir e informar a los encargados de la infraestructura, para que sean estos quienes puedan confirmar o desechar el reporte
Artículo 16.	La supervisión del plan de respuesta frente a incidentes o recuperación ante desastres desde el punto de vista TI y de Ciberseguridad, hoy convergen en el concepto de Ciberesiliente. La Ciberresiliencia es la capacidad de prepararse, responder y recuperarse de los ataques cibernéticos. Considero importante tambien, incorporar el concepto de Gobernanza TI En base al estándar NIST, el ciclo debería considerar las 5 etapas: Identifiar, Proteger, Detectar, Responder y Recuperar.