Bogotá, septiembre de 2024

"Ataques a Cables Submarinos. Continuidad de operaciones crítica"

Así como se vivió una situación extrema y no avizorada con el implando COVID 21 que devino en atender situaciones que no se habían previsto, estamos ad portas de vivir un evento catastrófico de similares o peores características. El complejo entramado de cables de fibra óptica submarinos que transfieren datos entre continentes ha sido objeto de amenaza por parte de Rusia que identifica este sistema de comunicación como un objetivo militar legítimo que puede afectar los países occidentales.

Y es que, en definitiva, estos cables son realmente susceptibles de acciones hostiles por su alto nivel de vulnerabilidad. Se trata de más de 1.000 millones de metros de cable submarino que diferentes empresas llevan instalando desde 1866 (inicialmente para comunicación por telégrafo) para transportar datos entre continentes. Aunque tendemos a creer que nuestra comunicación se realiza principalmente a través de satélites, la implementación de la fibra óptica ha ganado terreno debido a la reducción de costos. Si la malla submarina fuera atacada o dañada gravemente, se perdería un acceso significativo a los servicios de internet, que consideramos fundamentales para nuestras economías, como las llamadas, las transacciones financieras y el streaming.

No obstante, las amenazas a esta infraestructura crítica provienen de unos pocos países clave, el problema se ha intensificado con las crecientes amenazas rusas, como las proferidas este año por Dmitry Medvédev, vicepresidente del Consejo de Seguridad de Rusia, contra el sistema de cableado; sin embargo, las amenazas a esta infraestructura crítica provienen de unos pocos países clave, el problema se ha intensificado con las crecientes amenazas, como las proferidas este año por Dmitry Medvédev, vicepresidente del Consejo de Seguridad de Rusia, contra el sistema de cableado.

Comandantes, analistas y estrategas militares, como el jefe de inteligencia de la OTAN, David Cattler, han advertido sobre el peligro cada vez más real de un ataque ruso a esta infraestructura en represalia por el apoyo de Occidente a Ucrania en la llamada "operación militar especial" lanzada por

Rusia en febrero de 2022 contra su vecino. De esta amenaza real existen precedentes de ataques a cables submarinos como el incidente en 2023 cuando un cable de telecomunicaciones que atraviesa el mar Báltico fue saboteado, atribuido a una "fuerza externa o manipulación", según Carl-Oskar Bohlin, ministro de Defensa Civil de Suecia.

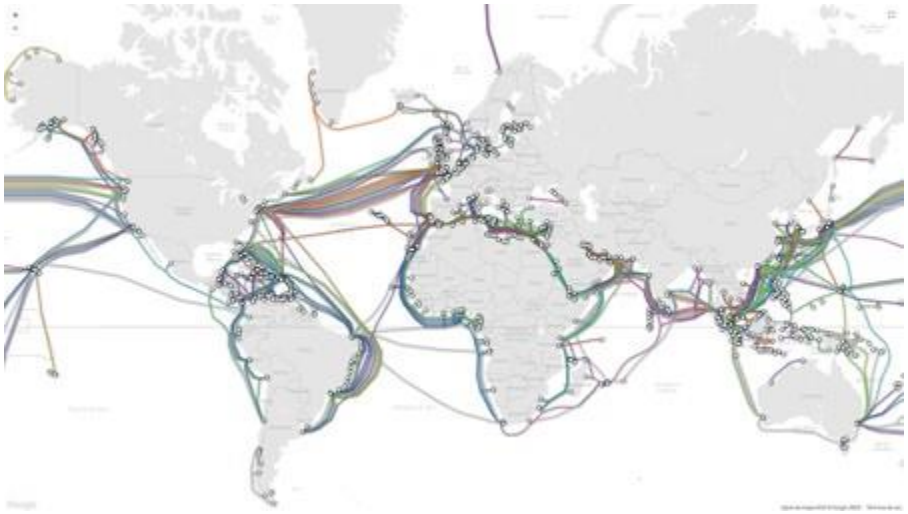

Imagen 1. Cable de fibra óptica submarino.
Fuente:https://www.nobbot.com/cable-submarino-internet-mundo/

Como se ha señalado, los cables submarinos de internet son esenciales para la conectividad global, ya que transportan la mayor parte del tráfico de datos entre continentes. En el caso de la conexión Europa- América, esta se efectúa a través de 17 cables que, si se obstruyen o se dañan, pueden generar consecuencias significativas como interrupciones en la conectividad, impacto económico, problemas de comunicación, riesgos para la seguridad, diversificación y redundancia**.** En resumen, aunque la obstrucción de los cables submarinos puede causar problemas serios, la red global está diseñada para ser resiliente y manejar tales eventualidades de manera efectiva.

Sin embargo, a la luz de la norma ISO 22301 que, como es sabido, se centra en la gestión de la continuidad del negocio, proporcionando un marco para que las organizaciones se preparen, respondan y se recuperen de incidentes disruptivos, en el caso de un ataque a un cable conector submarino entre América y Europa, se pueden adoptar varias medidas dentro del contexto de esta norma. Para que Colombia se prepare ante la contingencia de un probable ataque a un cable submarino de fibra óptica, es crucial adoptar un enfoque integral que abarque medidas de preparación, respuesta y

recuperación, alineadas con la norma ISO citada. Se ponen en consideración algunas medidas estratégicas, obviamente muy limitadas, que las autoridades involucradas en el tema podrían analizar eventualmente y que el lector puede evaluar, mejorar y profundizar:

Sobre **medidas de preparación**, se requiere identificar los servicios críticos, evaluar los servicios esenciales e infraestructura crítica que dependen de la conectividad internacional, como la banca, telecomunicaciones y servicios de internet; así mismo, determinar el impacto potencial de cómo la interrupción afectaría la economía y la seguridad nacional.

Al efectuar la evaluación de riesgos, es importante determinar las amenazas y vulnerabilidades; se requiere consultar evaluaciones periódicas de identificación de amenazas específicas a los cables submarinos y vulnerabilidades en la infraestructura efectuadas por países europeos, norteamericanos o de entidades multinacionales como la Unión Europea o la OTAN, considerando la probabilidad de ataques cibernéticos simultáneos que puedan agravar la situación.

Otro acápite especial se debe orientar a generar estrategias es crear planes que incluyan el uso de redes satelitales y proveedores de servicios de internet redundantes, incluyendo la inclusión de simulacros y entrenamientos regulares para asegurar que los actores involucrados estén preparados para participar ante riesgos materializados.

En torno a las **medidas de respuesta**, se sugiere contar con un plan que considere la ejecución inmediata de este plan de respuesta a incidentes una vez se detecte una interrupción del servicio. Aquí es determinante contar con rutas de comunicación alternativas o redundantes para mantener la continuidad de los servicios como ya se ha expresado.

La comunicación efectiva se constituye en un factor clave, para lo que se debe contar con canales claros, definidos, verificados que mantengan vinculadas a todas las partes interesadas interna y externa.

En este mismo sentido, la coordinación con actores clave, públicos y privados previamente identificados de sectores como telecomunicaciones y autoridades responsables de infraestructura crítica nacional, es necesaria para solicitar a otras naciones y empresas globales la restauración de la conectividad en el menor tiempo posible, para lo cual se puede contribuir con recursos disponibles como el intercambio de información con otras

empresas y organismos de seguridad sobre temas como amenazas, experiencia y mejores prácticas.

Respecto de las **medidas de recuperación**, y conforme a la gradualidad de reconexión del servicio, establecer un protocolo para dar prioridad a los servicios más críticos sin dejar de ofrecer soluciones temporales como el uso de redes satelitales.

Como señalan diferentes protocolos y normas, la evaluación Post-Incidente no puede ser obviada y demanda el análisis exhaustivo y detallado del incidente, así como una evaluación para identificar lecciones aprendidas que deben documentar los hallazgos y ajustar los planes de continuidad y respuesta para, finalmente, revisar y actualización los planes de continuidad del servicio y los procedimientos de respuesta basados en la experiencia del incidente.

Por último, ya considerados los niveles estratégicos, la sugerencia es generar, en todos los sectores productivos del país, planes de contingencia fundados en la norma ISO 22301, mencionada anteriormente y las normas de la familia ISO concomitantes. De igual manera, se pueden consultar normas como la **NIST SP 800-34** del Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST), la norma **ASIS SPC.1-2009** de ASIS International, entre otras reglas que abordan el tema.

My (RP) **Héctor Castro Corredor**
Administrador Policial.
Especialista en seguridad, investigación criminal y alta gerencia.
Consultor SVSP, Miembro colegiado COLPAP.

Bibliografía

Bevan, T. (2023). *Guía de implantación de la continuidad de negocio ISO 22301:2019.*

Europa Press Internacional. (14 de Julio de 2023). *Rusia amenaza con destruir los cables de comunicación submarinos de los "enemigos" occidentales.* Obtenido de europapress.es: https://www.europapress.es/internacional/noticia-rusia-amenaza-destruir-cables-comunicacion-submarinos-enemigos-occidentales-20230614114753.html

Fernández, Y. (19 de Enero de 2018). *Así es el mapa de todos los cables submarinos que le dan forma a Internet*. Obtenido de xataka.com: https://www.xataka.com/otros/asi-es-el-mapa-de-todos-los-cables-submarinos-que-le-dan-forma-a-internet

Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST). (2021). *NIST Special Publication (SP) 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems.* Abril: 23.

Organización Internacional de Normalización. (2019). *Norma ISO 22301.* Ginebra, Suiza.

Porter, T. (04 de Abril de 29). *Rusia amenaza con destruir los cables que sostienen internet y el sistema GPS: Occidente no tiene un buen plan de emergencia.* Obtenido de businessinsider.es: https://www.businessinsider.es/rusia-amenaza-destruir-cables-sostienen-internet-sistema-gps-occidente-no-tiene-buen-plan-emergencia-1402176

Prensa Alternativa. (05 de Septiembre de 2024). *Los rusos le dieron a Occidente donde más le duele*. Obtenido de @prensa-alternativa : https://www.youtube.com/watch?v=YyN2RsQr48k

Redacción HuffPost. (07 de Julio de 2023). *Europa teme un ataque ruso a los cables submarinos*. Obtenido de huffingtonpost.es: https://www.huffingtonpost.es/global/europa-teme-ataque-ruso-cables-submarinos.html#:~:text=Est%C3%A1n%20trabajando%20para%20vigilar%20y%20reconocer%20todas%20las

The Economist. (12 de Julio de 2024). *Cómo China y Rusia amenazan el suministro de Internet a nivel global.* Obtenido de infobae.com: https://www.infobae.com/economist/2024/07/13/como-china-y-rusia-amenazan-el-suministro-de-internet-a-nivel-global/#:~:text=Un%20informe%20publicado%20en%20febrero%20por%20Policy%20Exchange,

Vega, F. (19 de Agosto de 2023). *La guerra secreta de cables submarinos*. Obtenido de @recent-platzi: https://www.youtube.com/watch?v=2j6XKpRyIrc

Viso, Z. (19 de mayo de 2017). *Descubre el mapa de cables submarinos que conectan el mundo*. Obtenido de https://www.nobbot.com/: https://www.nobbot.com/cable-submarino-internet-mundo/