CERC

Powered by METABASE Q

Consejo de Expertos en Regulación y Ciberseguridad

Ciberseguridad en Tiempos de Guerra

ÍNDICE

Elaborado por: Liliana Jiménez, Diego Rodríguez Henry, Gloria Valencia, Mariana Gómez, Monserrat Peña, Anahí Lima, Louise Ireland, Mauricio Benavides, consejeras y consejeros del Consejo de Expertos en Regulación y Ciberseguridad (CERC).

Este documento, elaborado por las consejeras y los consejeros del Consejo de Expertos en Regulación y Ciberseguridad (CERC), te brindará información relevante sobre el panorama actual de la ciberseguridad y del entorno digital en México y en el mundo.

Serás consciente de las prácticas maliciosas y vulnerabilidades a las que todos estamos expuestos, así como de las soluciones. Encontrarás recomendaciones para tener en cuenta en tu entorno; tu lugar de trabajo, tu casa y en tus dispositivos personales.

¿A QUÉ NOS REFERIMOS CON "TIEMPOS DE GUERRA"?

Si bien pareciera que los conflictos bélicos en el mundo están lejos de nuestra puerta, la realidad es que tienen implicaciones en nuestro entorno diario. Queremos fomentar la conciencia sobre la relevancia de la ciberseguridad en todo el mundo y en nuestras vidas. A medida que nuestro mundo digital y físico están cada vez más conectados, los conflictos también han traspasado las fronteras físicas para llegar a las digitales.

Actualmente, vivimos la integración del Internet como una extensión de nuestra vida, que originalmente nació de la necesidad de obtener un conjunto descentralizado de redes de comunicación. Esto, además de todas sus ventajas en el desarrollo tecnológico y de las comunicaciones, trajo riesgos. La posibilidad de terceros que interfirieren en el intercambio de la información genera la necesidad de seguridad y protección.

Uno de los primeros ciberataques registrados, que demostró el potencial de impacto de esta técnica, se remonta a la década de los años 90, cuando un grupo conformado por más de 450 expertos informáticos de diferentes nacionalidades lograron acceder a información estratégica de la Organización del Tratado del Atlántico Norte (OTAN) y bloquearon la web de la Casa Blanca durante un fin de semana.

Para entender qué es la ciberseguridad, la Unión Internacional de Telecomunicaciones (UIT), el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), la define como: "El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación,

prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y usuarios en el ciberentorno".

Asimismo, en el CERC consideramos que la ciberseguridad es un asunto de ética que nos compete a todos. Es una responsabilidad compartida, que involucra al sector público, al sector privado, a las organizaciones sociales, a la academia, a la sociedad en general, a ti y a mí. Necesitamos un cambio de paradigma que nos permita transitar de un enfoque reactivo e individual, hacia una defensa colectiva enfocada en la prevención.

Nos referimos a "tiempos de guerra" a toda aquella circunstancia en la que se involucra siempre a un atacante y que requiere de un sistema de defensa, preventivo o reactivo; de cualquier naturaleza: bélica, corporativa, gubernamental, entre otros.

CONTEXTO ACTUAL

Durante la pandemia ocasionada por el COVID-19, la digitalización ha tomado más espacios, es por ello que nuestro patrón de comportamiento debe observar los riesgos que pueden presentarse. La pandemia aceleró cinco veces el desarrollo tecnológico previsto para esta época.

Nuestra exposición y las vulnerabilidades en la seguridad nos concierne a todos, lo cual se ve reflejado en el incremento de ciberataques, como podrás observar en los siguientes datos:

Figura 1. Contexto actual de la ciberseguridad

¿CÓMO ACTÚAN LOS CIBERATACANTES?

Suelen ser personas creativas, curiosas, con mucha imaginación y que utilizan todas estas características de forma maliciosa para llevar a cabo sus ataques. Pueden estar en cualquier rincón del mundo, atravesar fronteras físicas, penetrar en sistemas de grandes empresas trasnacionales, hasta cualquiera de tus dispositivos con acceso a Internet.

Se calcula que en 2021 los delitos cibernéticos infringieron daños por $6 billones de dólares a nivel mundial y se espera que los costos incrementen un 15% anual, hasta llegar a $10.5 billones de dólares en 2025. Al comparar los $3 billones de dólares que costaba en 2015, esto representa la mayor transferencia de riqueza en la historia, de acuerdo con el reporte de "*The CEO's Guide to Data Security*" de *AT&T Cybersecurity Insights*.

Aunado a esto, muchos individuos se unen a cibergrupos clandestinos maliciosos, así catalogados por la BBC, como Guacamaya y Raccoon.

BUENAS PRÁCTICAS INTERNACIONALES

2004
UNIÓN EUROPEA

Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés)
Objetivo: Promover la política de seguridad cibernética de la región, la fiabilidad de los productos, servicios y procesos de Tecnologías de la Información y Comunicación (TICs), cooperación Estados miembros y organismos de la UE, y preparación para los desafíos del en materia de ciberseguridad.

2016
REINO UNIDO

Centro Nacional de Ciberseguridad (NCSC, por sus siglas en inglés)
Objetivo: Ofrecer un punto de contacto único para PyMEs, grandes organizaciones, agencias de gobierno y el público en general

2016
ESPAÑA

Instituto Nacional de Ciberseguridad (INCIBE)
Objetivo: Afianzar la confianza digital, elevar la ciberseguridad, la resiliencia y al uso seguro del ciberespacio en dicho país.

2018
ESTADOS UNIDOS

Agencia de Seguridad Cibernética e Infraestructura (CISA, por sus siglas en inglés)
Objetivo: Comprender, administrar y reducir el riesgo cibernético a nivel nacional

ESTONIA

A pesar de ser un país con solo 1.3 millones de habitantes, Estonia cuenta con una de las infraestructuras de defensa cibernética más sólidas del mundo, estando solo detrás de Estados Unidos.

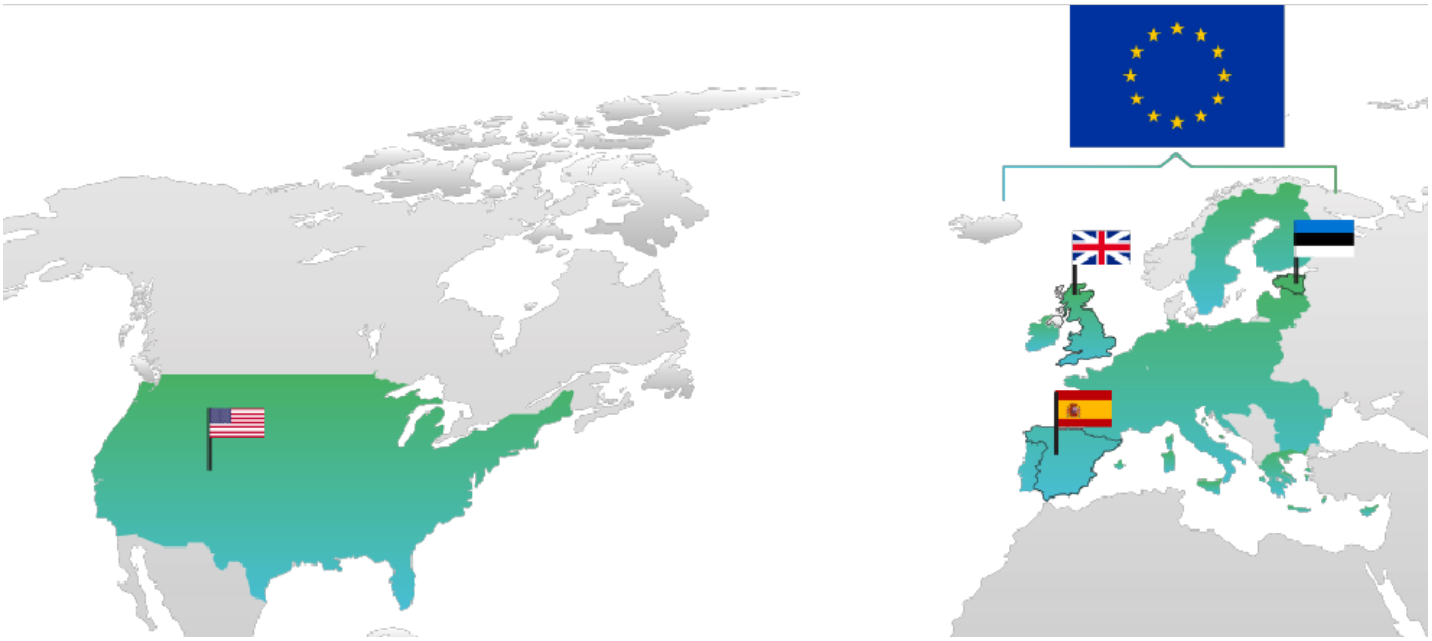

Figura 2. Buenas prácticas internacionales

LA MAGNITUD DE LOS CIBERATAQUES

Cuando un ciberataque o una serie de ataques es dirigido a un país, hablamos de una ciberguerra, debido a que tienen el potencial de causar estragos en la infraestructura gubernamental y civil, lo cual provoca daños no solo al Estado, sino incluso la pérdida de vidas.

En la ciberguerra, las fronteras son inexistentes y los atacantes pueden permanecer en el anonimato. Si desglosamos la palabra ciberguerra, tenemos tres componentes: computadoras, comunicaciones y guerra.

El objetivo de los ciberatacantes es desmantelar o deshabilitar la infraestructura informática del enemigo, al bloquear accesos, ocasionar retrasos en la red, provocar denegación de servicios, lanzar *malware* masivamente (*spyware,* virus, gusanos, troyanos), crear *botnets*, y robar información. Por lo tanto, incluir el componente de ciberseguridad al análisis de los conflictos bélicos es fundamental. Tal es el caso más reciente entre Rusia y Ucrania.

Las tensiones históricas entre estos países se intensificaron en 2014 con la declaratoria de Vladimir Putin sobre la anexión de Crimea a Rusia, tras el movimiento separatista en la región. En mayo del mismo año, desde Rusia se llevó a cabo un ciberataque que buscaba incidir en la elección presidencial de Ucrania, que consistió en un malware diseñado para infiltrarse en la red central del sistema electoral a fin de elegir al presidente de ese país y borrar archivos que dejaran el sistema de votos inservible. El ataque fue identificado y eliminado, sin embargo, tuvo implicaciones en el conteo de votos y generó desinformación sobre los resultados.

En años posteriores, continuaron los ciberataques al sector energético de Ucrania que afectaron a miles de personas. En 2017, hubo otro ciberataque el cual se adjudicaron ciberatacantes rusos quienes utilizaron "*NotPetya Ransomware + wiper*", conocido como el ataque más devastador de la historia, el cual afectó al 80% de sistemas privados y públicos, de los sectores energético y financiero. Después, este *malware* se expandió a 65 países, el cual afectó un total de 49,000 sistemas.

Contrario a muchas de las primeras posturas de los analistas sobre el conflicto, la defensa colectiva que fueron capaces de orquestar los ucranianos, desde un llamado abierto de su

presidente Zelensky, demostró ser más fuerte que las capacidades cibernéticas ofensivas de los rusos, quienes lanzaron una intensa campaña de ciberataques (800 ataques contra objetivos ucranianos, durante los primeros días del conflicto).

Es evidente que el conflicto entre ambos países ha escalado y no solo se ha quedado en el plano político, también ha tenido una repercusión en diferentes ámbitos que han terminado por afectar a otras regiones. Saber cómo piensa y cómo está organizado el enemigo es fundamental en cualquier guerra. Conocer sus tácticas y técnicas, sus medios y recursos, los canales de comunicación, ubicaciones estratégicas y sus aliados.

El conflicto entre Rusia y Ucrania es la primera gran confrontación entre dos potencias tecnológicamente avanzadas en la era cibernética. Nos incita a cuestionar la naturaleza de la guerra moderna y el papel del ciberespacio.

LA ACCIÓN COLABORATIVA PARA ENFRENTAR UN CIBERATAQUE

"Un ataque a un miembro de la OTAN representa un ataque a todos los miembros de la organización". Este es el principio rector de la Organización del Tratado del Atlántico Norte (OTAN), en su artículo 5º, el cual ha sido la piedra angular de esta alianza.

De acuerdo con el *Global Cybersecurity Outlook* 2023 del Foro Económico Mundial, los líderes empresariales, los jefes de seguridad informática y los miembros de los consejos de administración ahora coinciden en que los riesgos cibernéticos están relacionados con la inestabilidad geopolítica. Se realizan esfuerzos para reforzar las políticas y procesos internos, así como para aumentar la eficacia de los controles de ciberseguridad con terceros.

La situación geopolítica derivada del conflicto entre Rusia y Ucrania también ha alterado nuestra forma de concebir el entorno de las amenazas. Hemos tenido que dedicar tiempo y recursos a comprender cómo ha cambiado el panorama. Ahora dedicamos más recursos a la vigilancia activa, nos centramos en nuestra planificación táctica a corto plazo (tres meses) y somos menos meticulosos en nuestra planificación de mediano y largo plazo (cuatro a doce meses), ya que el entorno se ha vuelto muy volátil, puntualiza el reporte.

El conflicto destaca, una vez más, la importancia de la ciberseguridad. Hoy en día, a nivel global, nos desplazamos y actuamos en el entorno digital, lo cual representa muchas ventajas, pero también riesgos y desafíos para los que nos debemos preparar.

Un ciberataque exitoso puede representar pérdidas económicas, de información, de productividad y hasta de reputación. Generalmente, se ha entendido a la defensa desde un punto de vista y acción individual, lo cual ya no tiene sentido. El crimen ha evolucionado, como lo hemos visto en este documento, ahora los ciberatacantes actúan en colectivo. Es por ello que la defensa tiene que ser desde un enfoque colaborativo y ofensivo, con inteligencia, conciencia, información y preparación para prevenir, mitigar y responder efectivamente.

En el caso referido de Ucrania, cuando solicitó asistencia a su gente, sus aliados y al mundo para la defensa cibernética, inmediatamente se hizo evidente que la capacidad para operar en el ciberespacio no solo dependía de las agencias gubernamentales y militares, sino también de la estrecha colaboración de las empresas comerciales de tecnología y ciberseguridad y la empatía de gurús informáticos alrededor del mundo. En este contexto, muchos actores decidieron asumir roles proactivos en la defensa de Ucrania, y han resultado fundamentales en el conflicto.

Como se ha podido observar, la acción colaborativa ha resultado crucial en la capacidad de defensa y respuesta ucraniana; no obstante, la ciberguerra también ocurre en “tiempos de paz”, como una especie de guerra fría, en constante espionaje y sabotaje. En dicho escenario, también la cooperación es un elemento vital, y debe incluir a los sectores público y privado, así como al público en general para la concientización.

Para que los países y las organizaciones participen en esquemas de defensa efectiva, la primera línea de defensa es adoptar un enfoque distinto, de manera colectiva, priorizando el intercambio de información. Es fundamental reunirnos, por sectores, giros, grupos, o como se considere necesario, y pensar en soluciones en colectivo. Debemos confiar el uno en el otro, eso nos hace más fuertes y resilientes. Todos tenemos un grado de recelo respecto a nuestra información, pero es necesario pensar en el bien mayor, construir sobre una base de confianza por el bien colectivo.

Existen diversos niveles y metodologías en la práctica de la Defensa Colectiva. En el primer nivel, y aunque es un nivel útil para intercambiar técnicas sobre la mejor manera de responder a los ataques, es un enfoque más reactivo que proactivo. Pocas organizaciones disponen de sistemas para compartir información de forma eficiente y ganar la batalla a los ciberatacantes.

El siguiente nivel hacia una Defensa Colectiva efectiva son las políticas compartidas; normas mínimas de ciberseguridad, los recursos y la investigación para defenderse de los ciberataques. Actualmente, éste se lleva a cabo principalmente en algunas organizaciones y esferas de gobierno en Estados Unidos y países miembros de la Unión Europea. Este nivel permite mayor compenetración entre los miembros, existe un mayor intercambio de información. Cada parte en lo individual mejora su ciberseguridad, aunque se mantienen ciertas brechas, que ante ciberataques certeros y con alto grado de agresividad, no les permite actuar eficazmente como un conjunto colectivo.

En un tercer nivel, las entidades gubernamentales y las industrias entran en un esfuerzo conjunto más profundo por lograr una mayor colaboración entre los sectores público y privado; este modelo ya se lleva a cabo en algunas regiones dentro de Estados Unidos. La implementación exitosa de la Defensa Colectiva permite una mejor preparación y respuestas más rápidas a los ciberataques.

Para ello, sería más eficaz contar con una entidad independiente, que administre confidencialmente los datos de las distintas partes, a fin de defenderse de los ciberataques. Si los sistemas se comunican entre sí, es más sencillo prevenir las amenazas y adoptar un enfoque ofensivo.

Los ciberatacantes siempre han tenido la ventaja. Debemos cambiar esto mediante un enfoque colectivo de defensa. La misión es hacer crecer una comunidad diversa de organizaciones que tienen en común un compromiso con la ciberseguridad y que pretenden mejorar la seguridad nacional e industrial a través de la Defensa Colectiva. A través de este intercambio multi direccional, se ayuda a las organizaciones a gestionar los riesgos de sus negocios y la comunidad.

Para enfrentar este desafío, es necesario atender a aquellas iniciativas que faciliten la inteligencia, los recursos de resiliencia y una red de confianza de expertos internacionales a fin de anticipar, mitigar y responder a las amenazas de ciberseguridad.

DEL IMPACTO GLOBAL AL PERSONAL

¿Cómo nos impacta lo anterior como individuos? Así como no podemos tener misiles en la azotea de nuestras casas para defendernos, es igual de difícil para cualquier persona u organización defenderse de un ciberataque a infraestructuras críticas. Sabemos que el Estado debe ser garante de nuestra seguridad, sin embargo, para ello se requiere un marco regulatorio sólido e innovador, que garantice nuestros derechos y obligaciones, que tome en cuenta la delgada línea entre la libertad y la seguridad.

Existe la creencia de que nuestra información no es relevante para los ciberatacantes; no obstante, el acceso a nuestros patrones de conducta, información sobre nuestra identidad y patrimonio, pueden resultar de su interés, o incluso utilizarnos como peones en un ataque a mayor escala. De ahí la importancia de generar conciencia a todos los niveles sobre la situación.

REFLEXIÓN

Es importante hacer conciencia de la íntima relación entre lo que ocurre en el mundo físico como en el virtual. Así sea una pandemia como la ocasionada por el COVID-19, un conflicto internacional o un ciberataque, la amenaza puede venir desde cualquier parte del planeta y sorprendernos en el momento menos esperado. Por lo tanto, la prevención es nuestra mejor defensa. En este sentido, es importante responder a la pregunta: ¿de qué manera podemos estar preparados?

El caso entre Rusia y Ucrania nos deja ver que un ciberataque tiene el potencial de causar estragos en la infraestructura crítica de un país, al provocar daños no solo al Estado, sino también puede representar daños a nuestro entorno cotidiano, materializándose en pérdidas económicas, de información, de productividad y de reputación en organizaciones e individuos.

Para evitarlo, se pueden emprender muchas prácticas desde nuestros propios ámbitos de acción, empezando por promover la concientización de ciberseguridad en nuestro entorno. Por otra parte, la importancia de atender las recomendaciones de especialistas: contar con una higiene digital básica, cambiar nuestras contraseñas frecuentemente, cuidar la información que

se comparte en Internet, revisar los términos y condiciones de las aplicaciones y mantener actualizados nuestros dispositivos.

En el CERC consideramos que México puede contar con estrategia adecuada de ciberseguridad al establecer un marco regulatorio sólido e innovador, mantener un proceso permanente de concientización que promueva la colaboración entre instituciones públicas y privadas, sociedad civil y academia, sin dejar de atender a la posible adopción de las mejores prácticas internacionales y la cooperación entre todos los involucrados.

Actuemos en colectivo. Cuando tu seguridad funciona, tu futuro funciona.

REFERENCIAS

1. Agencia de la Unión Europea para la Ciberseguridad (ENISA), Unión Europea: https://www.enisa.europa.eu/about-enisa/about-enisa-the-european-union-agency-for-cybersecurity
2. Aon comparte cinco estrategias para mitigar incidentes de ciberseguridad, Reseller Redactores: https://reseller.com.mx/aon-comparte-cinco-estrategias-para-mitigar-incidentes-de-ciberseguridad/
3. BBC noticias, mundo, sección América Latina: https://www.bbc.com/mundo/noticias-america-latina-63098421
4. Beecroft, Nick. Evaluación del apoyo internacional a la defensa cibernética ucraniana, Carnegie Endowment for International Peace: https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322
5. Ciberataques, la mayor amenaza actual, Instituto Español de Estudios Estratégicos, 09/2015: https://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf
6. Cybercrime To Cost the World $10.5 Trillion Annually By 2025, Cybercrime magazine: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
7. Ciberguerra: la nueva amenaza global: https://www.youtube.com/watch?v=Le9wh5AH0IE&t=1440s
8. Cybersecurity and Infrastructure Security Agency (CISA), United States of America: https://www.cisa.gov/sites/default/files/publications/CISA-Factsheet_16-Dec-2021-V4_508.pdf
9. Digital Consumer Survey Mexico 2020, Nielsen: https://www.nielsenibope.com/2020/09/14/digital-consumer-survey-mexico-2020/
10. Encuesta Nacional de Consumo de Contenidos Audiovisuales 2022, Instituto Federal de Telecomunicaciones: https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/en-mexico-se-consumen-25-horas-de-tv-abierta-y-3-horas-en-plataformas-de-video-en-internet-al-dia
11. Estonia golpeada por el ciberataque 'más extenso' desde 2007 en medio de tensiones con Rusia sobre la guerra de Ucrania, Euronews:

https://www.euronews.com/next/2022/08/18/estonia-hit-by-most-extensive-cyberattack-since-2007-amid-tensions-with-russia-over-ukrain

12. Global Cybersecurity Outlook 2023, INSIGHT REPORTJANUARY 2023, del Foro Económico Mundial: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf
13. HSBC, Clínica de ciberdelincuencia: cómo defender su empresa de los ciberdelincuentes: https://www.empresas.hsbc.com.mx/es-mx/insights/innovation-and-transformation/clinica-de-ciberdelincuencia-como-defender-su-empresa-de-los-ciberdelincuentes#:~:text=Debido%20a%20que%20los%20ciberataques,identidad%2C%20o%20malversaci%C3%B3n%20de%20fondos
14. Instituto Nacional de Ciberseguridad (INCIBE), España: https://www.incibe.es/que-es-incibe
15. National Cyber Security Centre, United Kingdom: https://www.ncsc.gov.uk/section/about-ncsc/what-we-do
16. Reporte "The CEO's Guide to Data Security" de AT&T Cybersecurity Insights, vol. 5: https://cybersecurityventures.com/wpcontent/uploads/2021/01/attceocyberreport_compressed.pdf
17. Security Week, The Lessons From Cyberwar, Cyber-in-War and Ukraine, https://www.securityweek.com/the-lessons-from-cyberwar-cyber-in-war-and-ukraine/?utm_campaign=Daily%20Newsletter&utm_medium=email&_hsmi=2&utm_content=2&utm_source=hs_email
18. Unión Internacional de Telecomunicaciones (UIT): https://www.itu.int/es/about/Pages/whatwedo.aspx